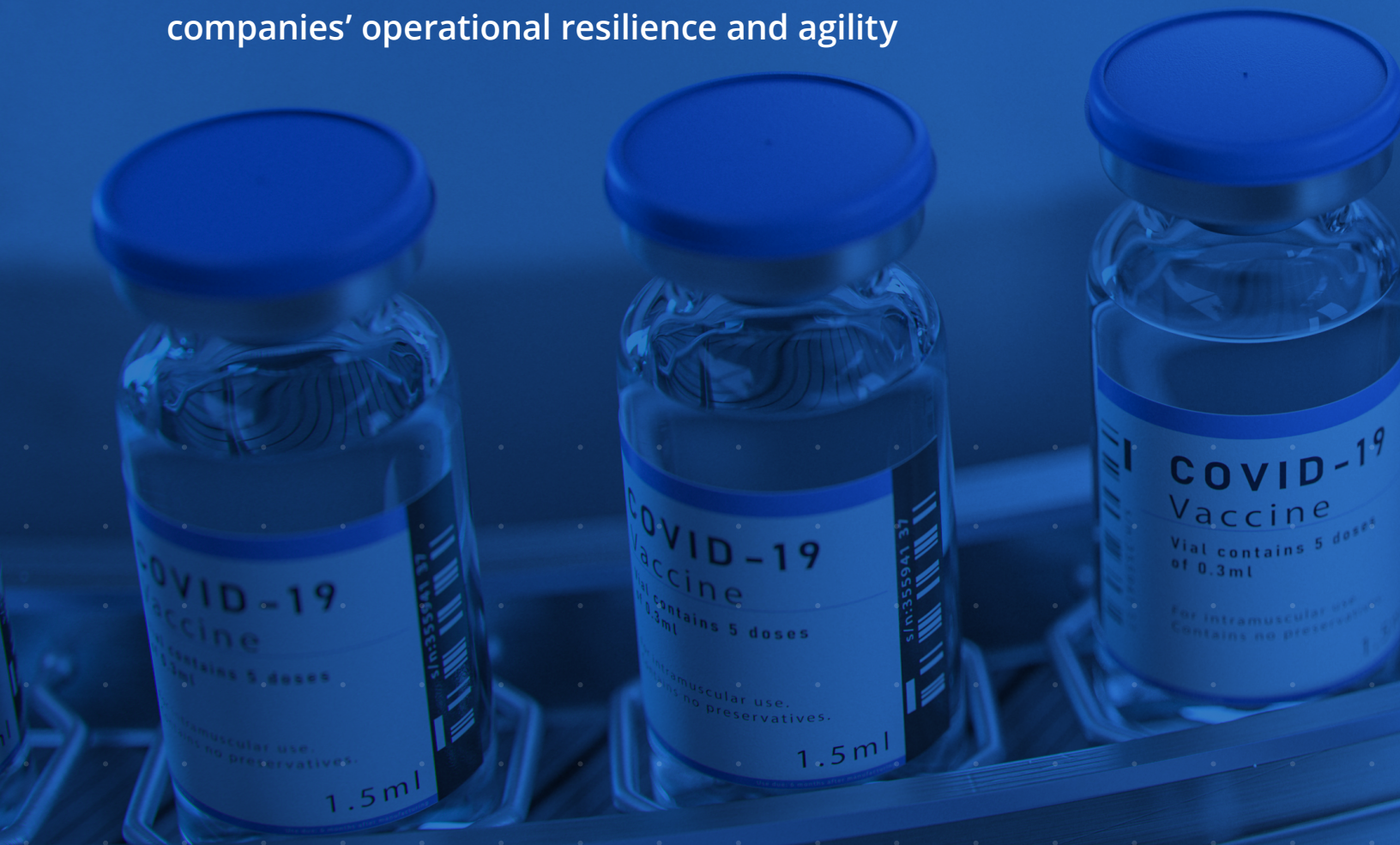# Pharma Risk Management

How lessons learned from the COVID-19 pandemic can strengthen pharmaceutical companies' operational resilience and agility

Dataminr®

At the height of the COVID-19 outbreak, many industries struggled to adapt to the operational changes and challenges brought about by the pandemic. But the pharmaceutical industry quickly sprang into action. It developed and delivered COVID-19 vaccines in record time. By December 2020, there were over **200 vaccine candidates** in development around the world.

While the pharmaceutical industry was able to deliver diagnostic tests, treatments and vaccines at an incredibly fast pace, the pandemic exposed how vulnerable the industry is to risks affecting digital and physical assets, as well as its supply chain.

In this ebook, we will address various aspects of the pharmaceutical industry that have been impacted over the course of the pandemic:

- Asset protection
- Cybersecurity
- Brand and reputation
- Supply chain

Asset Protection

Pharmaceutical companies have a great deal at stake when it comes to the safety and security of their physical assets. Most have thousands of facilities worldwide, with tens of thousands of staff and pieces of equipment. Unforeseen events and risks, such as natural disasters or bomb threats, can cause major disruptions and delays in production.

For example, in January 2021, a suspicious package was found outside a **Wockhardt, U.K., facility** that had partnered with global pharmaceutical giant AstraZeneca to fill 100 million vials of the COVID-19 vaccine The incident halted vaccine production as staff members were forced to evacuate the premises.

Physical threats to critical infrastructure are not the only dangers of which companies need to be aware. Accidents and failed safety protocols also have the potential to wreak havoc on production and distribution timelines, affecting supply for entire cities, states or even countries.

In March of 2021, **15 million doses of Johnson & Johnson's** (J&J) COVID-19 vaccine were contaminated due to human error at an Emergent BioSolutions plant in Baltimore, Maryland. This incident had an immediate effect on distribution—causing uncertainty for the production and shipment of over 24 million doses expected in April. Another human error at a Spanish manufacturer, Rovi, also caused **metal contaminants to get into Moderna** vials, which were shipped to Japan. After discovering the contamination in August, Japan had to suspend the use of nearly 2 million doses.

Stay Informed of the Latest Risk

Dataminr's real-time alerts inform customers when a high-impact event occurs and help to maintain their awareness as the situation unfolds. Customers were notified of the 5 Emergent BioSolutions vaccine contamination in real time, as well as key subsequent updates, including the Biden administration's response; the U.S. Food and Drug Administration (FDA)'s report on the facility; and the U.S. government canceling its contract with Emergent BioSolutions to produce J&J vaccines.

Another key lesson learned from the pandemic is that it's important to remember, even after a product leaves a lab or production facility, it's still vulnerable to several other risk factors. COVID-19 vaccine vials have been at risk of damage and destruction, even by some of the unlikeliest sources.

One of the most shocking examples is a **pharmacist who was arrested** for intentionally removing Moderna COVID-19 vaccines from a hospital refrigerator in Grafton, Wisconsin,

spoiling 570 doses. While healthcare workers were forced to dispose of those vaccines, it was revealed that 57 patients had received injections containing the spoiled doses.

The vaccines administered were rendered less effective or potentially ineffective, though fortunately none of the patients experienced adverse health effects. Though this incident was relatively isolated, it highlights the need for security and operational leaders to be aware of all forms of risk that can impact their physical assets.

Cybersecurity

It is apparent that the COVID-19 pandemic has accelerated the digitalization of many industries at an unprecedented rate. With new lockdown measures and social distancing restrictions, pharmaceutical companies swiftly began to move toward remote working and cloud-based systems. As such, securing their data has become much more critical.

However, all digital transformations come with inherent risks. These cloud-based hosting systems contain vital and sensitive data, such as health records, clinical trial records and intellectual property (IP), which, if compromised, could greatly jeopardize and threaten **healthcare** and pharmaceutical companies, as well as their

patients. Consequences can be staggering— ranging from stolen intellectual property, disrupted drug manufacturing and affected revenue to health data being used to blackmail and extort patients and/or organizations.

A prime example is when cyber criminals targeted multiple companies that were in the process of developing and testing their COVID-19 vaccines. Victims included the **European Medicines Agency (EMA)**, BioNTech, Pfizer, Moderna, J&J, AstraZeneca and Novavax. Hackers attempted or were able to access the companies' proprietary vaccine-related information in these cases—clear evidence that the pharmaceutical industry has quickly become an attractive and vulnerable target for cyber criminals.

Because cyber attacks on supply chains, in both R&D and manufacturing, are occurring more often and causing large-scale disruptions, pharma has come under renewed pressure to step up its cybersecurity measures.

Dataminr alerted its customers to all of the aforementioned attacks in real time, allowing customers' security leaders and teams to quickly assess the potential impact of the threats and address them accordingly—be it a patch, configuration change or system shutdown.

Mitigate Risk as Early as Possible

Dataminr's real-time information provides pharma companies with the earliest indications of cybersecurity vulnerabilities and threats across the surface, deep and dark web. On November 20, 2020, Dataminr provided the first publicly known indication that the EMA was vulnerable to a cyber attack more than two weeks before the agency disclosed it had been breached.

Brand and Reputation

The rapid rollout and success of COVID-19 vaccines have improved brand recognition and reputation for several pharmaceutical companies. Celebrities and politicians around the world have publicly endorsed the vaccines—from **Oprah Winfrey** and **Argentine Vice President Cristina Kirchner** to the **Dalai Lama**—strongly urging people to be inoculated.

However, in the meantime, the industry's image and credibility have also been affected by rampant misinformation and disinformation regarding the pandemic and vaccines. On July 17, 2021, U.S. President Biden told a group of reporters outside the White House that misinformation about COVID-19 vaccines is "killing people."

The World Health Organization (WHO) coined the term "infodemic" in the early stages of the pandemic to describe the unreliable reports and dangerous advice regarding the virus and treatments. For example, both **the WHO** and the FDA issued warnings against the use of ivermectin to treat COVID-19.

The situation remains a serious one as misinformation, disinformation and conspiracy theories continue to spread on various media channels. Not only does this put people's health and safety at risk, it negatively affects pharmaceutical companies' reputation.

Supply Chain

The pharmaceutical industry plays an integral role in the global supply chain of life-changing and life-saving medicines. At the same time, the safety and delivery of products are dependent on a globally dispersed and complex supply chain, as well as the integrity of R&D and manufacturing activities. This dependency presents various challenges when it comes to managing **supply chain risks**, especially due to the large number of parties involved in the manufacturing and distribution processes.

Numerous factors can impact the pharma supply chain, including natural disasters, **extreme weather,** civil unrest, workforce strikes and even traffic. For example, in February 2021, deadly winter storms across the U.S. delayed shipments of more than **six million COVID-19 vaccine doses**, affecting distribution and appointments in all 50 states.

Aside from the aforementioned cyber threats, economic, political and geographic disruptions are other potential risks that can derail production. Mitigating—or even preventing—these risks requires having the right information at the right time to make quick, well-informed decisions.

The Value of Real-Time Information

While many leading pharmaceutical companies have already started utilizing sophisticated artificial intelligence (AI) to enhance their capabilities in key data analysis areas, including supply chain risk, the challenges pharmaceutical leaders face are increasingly complex and dynamic. Many are turning to data—both their own and that which is external—to help them become more agile and resilient.

And, as we've learned from the pandemic, real-time information plays a critical role, especially in times of crisis or in the midst of unforeseen, high-impact events—from global supply chain disruptions and extreme weather to cyber attacks and civil unrest.

The real-time information that Dataminr provides, via Dataminr Pulse, gives customers a clear and early line of sight into the emerging risks and potential disruptions most relevant to them. As a result, they can more effectively mitigate risk and quickly respond, often before the threats are broadly communicated by media, governments, etc.

Billions of people worldwide rely on the pharmaceutical industry for life-saving medical products. By having the appropriate technology and security frameworks to stay ahead of, prepare for and mitigate risks, pharma companies can maintain business continuity and ensure minimal impacts on the public.

Learn more about the benefits of real-time information for the pharma industry.