www.PHARMAMANUFACTURING.com

pharma™ MANUFACTURING

THE DRUG INDUSTRY'S VOICE FOR MANUFACTURING EXCELLENCE

2021

Smart Pharma

SPONSORED BY

PutmanMedia®

Thermo Fisher
SCIENTIFIC

Biotech

Be ahead of the curve.

Is your process analytical technology ready for what's next?

Need to track batch progress in real-time? Increase product consistency? Learn how to gain productivity that is simple, data-rich and low-risk with Thermo Fisher Scientific. Processes can become more efficient, with reduced over-processing, and a greater product consistency.

Gain productivity by instituting a Process Analytical Technology program with Process Mass Spectrometry gas analysis.

Visit thermofisher.com/PAT to download our latest eBook, *A Guide to Improving Biotech Processes with Mass Spectrometry Gas Analysis*, product information or contact an application specialist today.

Learn more at **thermofisher.com/PAT**

TABLE OF CONTENTS

PRODUCT FOCUS

Every Drop Counts: Suite of new product inspection solutions addresses liquid pharma trends

Liquid pharma manufacturers are challenged with ensuring that they produce precise dosage sizes, and that the origin of their drugs is completely traceable through the supply chain. Both are critical in ensuring patient safety, to combat counterfeit medicines, as well as contributing to their own operational efficiency and reputation. Mettler-Toledo offers solutions that will help manufacturers to meet them: the Mettler-Toledo StarWeigh™ Checkweigher, for precision weighing of liquid pharmaceuticals; and the Mettler-Toledo T60 Integrated 360 Series, bringing advanced Track & Trace capabilities to the market for round objects such as bottles and vials.

The StarWeigh™ checkweigher provides laboratory accuracy of fill levels at production throughputs for small, instable or lightweight products, such as glass and plastic bottles, vials and ampules used in liquid pharmaceuticals. Up to four load cells can be fitted, including Mettler-Toledo's next-generation FlashCell™, capable of delivering highly accurate weighing results. StarWeigh™ is a compact checkweigher that can be installed within existing production lines and features customizable 'starwheels' to fit different package shape requirements and enable quick product changeovers.

The T60 Integrated 360 Series systems for Mark & Verify, Serialization and Aggregation of round objects such as bottles and vials helps manufacturers comply with regulatory demands. The T60 Integrated 360 Series offers the ability to control third-party systems that print codes directly onto bottles and vials versus the typical processes where bottles are inserted into cartons which are subsequently serialized. Manufacturers can save time and money by having fewer labeling and packaging processes.

METTLER TOLEDO Product Inspection | **(813) 889-9500** | **www.mt.com/pi**

aizon

AD INDEX

PRODUCT FOCUS

Dosing and filling pump that is compact and universally suitable for multiple industries

The latest product in the Hygienic series in the ViscoTec portfolio, the vipura-PUMP 10T dosing and filling pump, is suitable for pharma, food and cosmetics.

The compact design of the vipura-PUMP 10T makes it easy to integrate the dosing and filling pump into complete systems: The installation space length has been reduced by over 25% compared to pumps with the same dosing capacity; with a weight reduction of over 60%. At the same time, the dosing volume per revolution has been increased. The special dosing geometry ensures precise dosing results and short cycle times and works non-destructively, even with lumpy materials up to 20 mm in diameter. The dosing volumes can be flexibly adjusted – from 20 to 200 ml or even much higher, depending on the cycle rate. These quantities can be precisely dosed and filled, depending on the application, and matching the specific requirements.

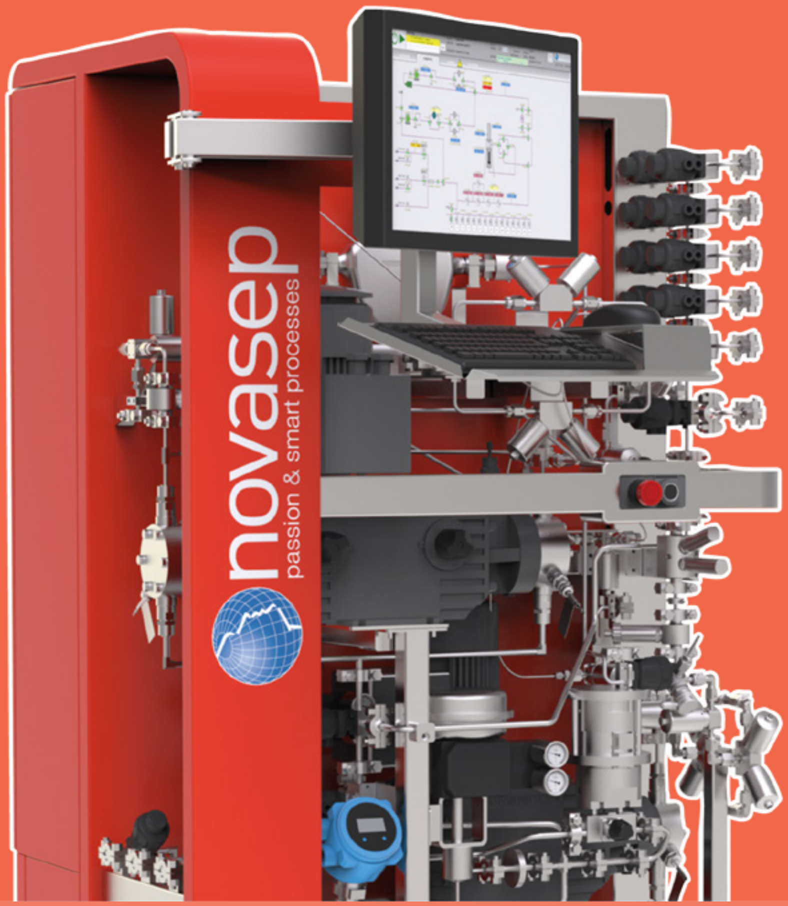
Due to its compact size and simple assembly/disassembly options, transportation of the vipura-PUMP 10T can be carried out by one person alone if required. Cleaning is simple and quick via a CIP connection.

The vipura-PUMP 10T is suitable for dosing and filling various materials: For food and pharmaceuticals, as well as household products and cosmetics. Common applications are, for example, tubular bag filling of chunky sauces or marinades, and of pet food or shower gel, detergents, toothpaste, creams, etc.

The benefits to you:

- Product change is made possible without disassembly
- One size fits all: For different dosing volumes
- Compact design + hygienic design in stainless steel
- Short cycle times
- Non-destructive dosing even of lumpy materials
- Transportation and cleaning can be done by 1 person
- Easy integration into existing systems

ViscoTec America Inc. | **(770) 422-4281** | **www.viscotec-america.com**


novasep
passion & smart processes

Cyber scares

The threats are real — and criminals are preying on pharma

By Karen Langhauser, Chief Content Director

Alan Brill didn't strike me as an alarmist. During our interview he was pleasant and calm, patiently explaining to me the ins and outs of cybersecurity.

But you shouldn't mistake Brill's composure for a lack of urgency.

With over 30 years of experience dealing with cybercrimes, Brill, who now serves as a senior managing director with Kroll's Cyber Risk practice, has been in some high-pressure situations.

In 1991, on the fifth day after coalition forces re-took Kuwait from the Iraqi army, Brill led a small team on the ground seeking intelligence from computers left behind by retreating Iraqi forces. In 2008, when a foreign intelligence service penetrated the computer networks of the Obama campaign, it was Brill who was tapped to lead the effort to remove the hackers and prevent them from re-entering.

So when Brill refers to the cybersecurity problem in the pharma industry as "existential," it's probably a good idea to take heed.

"This is a real issue. You can't simply say, 'Talk to the CIO, it's a technical problem' or 'Talk to the COO, it's an operations problem,'" says Brill. "It has come down to the fact that what you're dealing with is very often an existential problem — the company may live and die based on what happens."

And Brill is not the only one trying to get the word out.

Last year, the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) jointly issued a stark warning: China-affiliated cyber actors were caught trying to obtain valuable intellectual property and public health data related to COVID vaccines, treatments and testing. Pharma companies were among those targeted, and officials urged them to maintain dedicated cybersecurity because the delivery of treatment options — at a time when COVID was ravaging the world — was in jeopardy. Similar warnings have recently been sounded about hackers from both Russia and North Korea.

There is no shortage of data backing these warnings. According to a report from cyberthreat intelligence company BlueVoyant, cyberattacks on the biotech and pharma industry increased by 50% between 2019 and 2020.[1] Black Kite, a cyber-risk management company, recently found that one in 10 global pharma manufacturers are at a high risk of suffering a ransomware attack.[2]

Individual pharma companies are speaking out as well. During an online panel at the Aspen Cyber Summit last December, Johnson & Johnson's Chief Information Security Officer (CISO), Marene Allison, said J&J had seen a 30% uptick in cyberattacks

PRODUCT FOCUS

GxP AI Bioreactor Application helps pharma to scale manufacturing and quality

Aizon launches its Bioreactor Application, the pharma industry's first predictive analysis and deep knowledge management application. The Aizon Bioreactor Application adds the bioreactor process to the "Smart Manufacturing" transformation that is accelerating across the pharma and biotech industry. Aizon is uniquely able to achieve GxP compliance and provide an audit trail from the start of the process. The turnkey application allows pharmaceutical and biotech companies to leverage rich datasets generated during upstream manufacturing to detect and accurately predict deviations and outcomes — potentially leading to hundreds of millions of dollars in cost savings, reduced risk, and additional revenue upside.

Designed to work with both continuous and fed-batch bioreactors, the Aizon Bioreactor Application provides a deep understanding of the customer's bioprocess manufacturing lifecycle. The application leverages specialized Edge AI and contextualization, which is a requirement to make the data actionable. Contextualized data is harnessed, analyzed, and visualized through a persona-based lens for faster root cause analysis (RCA), real-time monitoring, and predictive insight across any number of bioreactor units and manufacturing sites.

Pharmaceutical and biotech companies can use the Aizon Bioreactor Application to further their digital transformation journey towards Pharma 4.0 and future-proof the path to continued process verification.

Aizon | **sales@aizon.ai** | **www.aizon.ai**

> “ As a professional in this field, I’m constantly amazed at the speed with which hackers adapt.
> — Alan Brill

during the pandemic and that health care organizations are fending off attempted penetrations by nation-state threat actors “every single minute of every single day.”

With many experts warning that the attacks on pharma are not only more frequent but more sophisticated, the message is clear: Cybersecurity threats have become a very real part of doing business in pharma and the industry’s continued success — as well as the lives of millions of patients — depend on pharma’s ability to kick its cyber vigilance into high gear.

THE LURE OF PHARMA

Among security professionals, 1930s bank robber Willie Sutton has become somewhat of a mythical figure. As the story goes (the incident was later refuted by Sutton himself in his autobiography), when a reporter asked the prolific thief why he robbed banks, Sutton replied, “because that’s where the money is.”

As one of the largest and most profitable industries in the world, pharma has long since been a darling of cybercriminals. To begin with, the industry is ripe with valuable intellectual property data on drug formulations and technologies.

“The ‘bad guys’ today know the pharma industry has trade secrets. The industry has information that they can monetize — that they can threaten to release and get money, or that they can encrypt and get money or some combination of the above,” says Brill.

The pharma industry is also the gatekeeper to massive amounts of personal health data collected during clinical trials. One analysis found that a patient’s full medical record can sell for up to $1,000 — nearly 10 times the going rate for social security numbers and credit card information.[3]

One of cybersecurity’s most cautionary tales involves the 2017 NotPetya ransomware attack that hit, among many organizations, Merck & Co. Often touted as one of the most devastating attacks in cyber history, the virus infected Merck through a server in Ukraine and quickly spread. The attack led to a disruption of worldwide operations, ultimately resulting in a $1.3 billion insurance claim.

Recent pharma-related cyber events

March 2020
U.S.-based CRO ExecuPharm revealed that "unknown individuals" deployed ransomware to its IT systems and sought payment for a decryption key. Attackers may have accessed and/or shared select personal information from ExecuPharm personnel, as well as from personnel at parent company, Parexel.

May 2020
The FBI and CISA issued a public service announcement warning health care, pharma and research sectors working on COVID response that they were the "prime targets" of hackers. Per the statement, China-affiliated cyber actors had "been observed attempting to identify and illicitly obtain valuable intellectual property and public health data."

May 2020
Several media sources reported that hackers linked to Iran targeted staff at Gilead Sciences, amid the company's scramble to develop COVID treatments. It was reported that hackers attempted to compromise email accounts of Gilead staff by using messages that impersonated journalists.

July 2020
The U.K.'s National Cyber Security Center revealed that a "cyberespionage group" associated with the Russian intelligence services attempted to hack into coronavirus vaccine research in the U.S., Britain and Canada.

July 2020
The U.S. DOJ indicted two Chinese men for spying on U.S. companies conducting coronavirus research. Prosecutors said that the hackers, who received some support from Chinese intelligence agents, had stolen "hundreds of millions of dollars' worth of trade secrets, intellectual property, and other valuable business information."

October 2020
Dr Reddy's Labs announced that it had isolated all its data centers in the wake of a cyberattack. The incident forced the Indian drugmaker to briefly shut down several production facilities in the U.S., U.K., Brazil, India and Russia, right as Dr. Reddy's was gearing up for late stage trials on Russia's Sputnik V vaccine.

November 2020
Sources told Reuters that North Korean hackers tried to break into AstraZeneca's systems as the drugmaker was working on its COVID vaccine. The hackers posed as recruiters on LinkedIn and WhatsApp to approach AstraZeneca staff with fake job offers, the sources said.

December 2020
WSJ reported that North Korean hackers targeted at least six pharma companies working on coronavirus treatments and vaccines in the U.S., U.K. and South Korea.

December 2020
IBM X-Force released a report on malicious cyber actors targeting the COVID cold chain. The phishing campaign spanned across six countries and targeted organizations working with Gavi, The Vaccine Alliance.

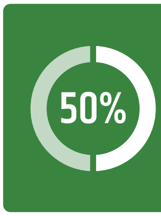
December 2020
Pfizer and BioNTech announced that documents related to the regulatory submission of their COVID vaccine had been accessed in a cyberattack on the European Medicines Agency. The EMA later confirmed that some of the stolen data was released online and Dutch newspaper De Volkskrant reported that both Russian and Chinese intelligence agencies were behind the attacks.

February 2021
South Korea's intelligence agency said North Korea attempted to steal information on coronavirus vaccines and treatments by hacking Pfizer.

March 2021
Cyber intelligence firm Cyfirma said that a Chinese state-backed hacking group targeted the IT infrastructure and supply chain software of two Indian vaccine makers — Bharat Biotech and the Serum Institute of India, the world's largest vaccine maker.

May 2021
The FBI and the Australian Cyber Security Centre warned of an ongoing global Avaddon ransomware-as-a-service campaign targeting multiple sectors, including the pharma industry.

* Dates correspond with when incidents were made public



Cyberattacks on the biotech and pharma industry increased by 50% between 2019 and 2020.

— BlueVoyant

As was the case with Merck, the global nature of the pharma industry makes it a broader target for cyberattacks.

"If I'm a criminal and I think I've found a weakness in your plant in Malaysia or your plant in Turkey or wherever, why not hit there?" says Brill. "It's all cyber-connected. They [cybercriminals] look for weak links — and they've gotten very efficient at exploiting them."

HITCH-HACKING PHARMA'S DIGITAL JOURNEY

Pharma Manufacturing's recent Smart Pharma Survey found a positive climate for digital innovation in the industry. Over 88% of respondents believe that, even if the manual processes used in their plants were seemingly effective, their companies would choose to automate processes if given the option. A similar percentage of respondents indicated that digitalization is an important part of the discussion when their companies are upgrading manufacturing facilities.

Digital innovations such as cloud computing, artificial intelligence and connectivity via industrial IoT are enhancing every aspect of pharma, from speeding up drug discovery to making plant floor operations easier and more efficient.

Despite all its benefits, digital transformation, if not handled carefully, also carries with it new cyber-risks.

For example, IBM Security's Cost of a Data Breach report found that misconfigured clouds were a leading cause of cyber breaches. For pharma, more than half of the industry's cyber incidents happen during this move to the cloud — and to make matters worse, breaches that happen during cloud migrations are the most expensive.[4]

While the pandemic has had a positive impact on pharma's digital progress, forcing the industry to drop a lot of its traditional constraints, it also has created more opportunity for cyberattacks.

"The pandemic undoubtedly exacerbated the rise of cyberattacks," says Liz Mann, EY Americas Life Sciences and Health Cybersecurity leader. "The shift to remote working facilitated an abrupt change to corporate network traffic patterns and to the degrees of controls implemented in a work-from-home environment."

Last year, hundreds of thousands of workers in the pharma industry pivoted to remote work virtually overnight, which resulted in, among many things, an influx of personal devices on corporate networks.

During Aspen's Cyber Summit, Meredith Harper, CISO at Eli Lilly, noted that the drugmaker's decision early on in the pandemic to allow some 16,000-17,000 global team members to work remotely substantially increased the footprint of the cyberattack surface.

According to Harper, Eli Lilly went to great lengths to quickly roll out an educational awareness program about how to better protect against cyberthreats in a home environment, including offering employees financial allowances to properly secure their workspaces.

The impact of the pandemic on cybersecurity wasn't exclusive to the pharma industry. Overall, the pandemic increased the threat of cyberattack for companies across all industries. Kroll and partners surveyed 500 security and risk leaders at large organizations — those with more than $500 million in revenue — on matters related to their cybersecurity programs, specifically threat detection and incident response. What they discovered was that the vast majority (93%) of organizations suffered a compromise of data over the past 12 months.[5]

NEW ATTACK MODELS

The pharma industry is frequently heralded for its life-saving innovations in human health. But like drugmakers, cybercriminals are also fast evolving.

"As a professional in this field, I'm constantly amazed at the speed with which hackers adapt and come up with new ways of working that actually work," reflects Brill. "You know, it's the kind of thing where if they would apply themselves to good things, we'd have great breakthroughs."

Wishful thinking aside, no industry is immune to attacks by nefarious actors, and despite its mission to save lives, this rule includes pharma. While it's concerning enough that attacks on pharma have become frequent, it's even more troubling that the attacks are more targeted and sophisticated.

While the ransomware approach with the end goal of financial gain remains the most popular method of attacking pharma companies, experts are warning that the spectrum of attacks is widening.

"The thing about cyberthreats is that old experiences fuel new ideas, and the landscape is always changing. Threat actors continue to demonstrate patience,

Ultimately, eliminating cyberattacks entirely is not possible, so it comes down to a familiar concept in pharma — managing risk.

creativity and determination in the process," says Mann.

Ransomware-plus

Ransomware — a form of malicious software ("malware") designed to block access to a computer system or data — makes up almost half of all reported attacks on the pharma industry.[1]

In its most basic form, ransomware works like this: Criminals encrypt a company's data or systems and then force the company to pay a ransom in exchange for decrypting the information or restoring access to systems.

But according to Brill, criminals have also started "double-dipping" in the ransomware pool.

"Kroll's internal intelligence group is seeing that in about half of our cases, before the ransomware is actually launched and everything is encrypted, the hackers steal the data," says Brill. "The hackers say, 'Pay me the ransom or you'll never get your data back.' And then after you pay the ransom, they say, 'By the way, I stole a copy of your data. And if you don't pay me more, it's going to be made public on the internet.'"

Brill says that Kroll has also recently seen an influx of attacks bypass the ransomware altogether. In these cases, attackers go beyond simply disabling systems; instead they steal sensitive data and hold it for ransom, threatening to sell it if the ransom isn't paid.

Digital espionage

Stories of suspected nation-state cyberespionage, sometimes reminiscent of old spy film plots, frequently light up the news headlines. Their intrigue is compounded by the fact that they are often shrouded in mystery — confirmed by "unnamed government sources" and lacking details regarding the perpetrators, whether the attacks were successful and what data may have been compromised.

Brill ran point on one of the most high-profile cases of suspected cyberespionage in history.

During the 2008 U.S. presidential election cycle, the FBI and U.S. Secret Service determined that both the Obama and the McCain campaigns were being targeted by hackers. A team of experts from Kroll, led by Brill, was dispatched to Obama's campaign headquarters and to the Democratic National Committee to identify the infection, cleanse infected systems and bolster defenses. Kroll investigators determined the compromise occurred through a phishing email made to look like the outline of a meeting agenda and containing a malicious .zip file attachment.

U.S. officials later attributed the attack to hacking units backed by the People's Republic of China. Dennis Blair, who served as President Obama's director of National Intelligence from 2009-2010, told NBC News that the hackers were, "looking for positions on China...surprises that might be rolled out by campaigns against China."

While espionage isn't the top cyberthreat faced by pharma companies, the pandemic has created an ideal scenario for nation-state attacks. The amount of valuable, proprietary information being generated by drugmakers during COVID vaccine development, combined with an international scramble for information and supplies, and the rise of vaccine nationalism, make vaccine data an almost irresistible target.

Early on in the pandemic, U.S. federal agencies accused both Chinese and Russian cyberespionage groups of attempting to steal COVID vaccine information from drugmakers.

Then, in December of last year — when the U.S. was just days away from authorizing its first vaccines — The Wall Street Journal reported that North Korean hackers targeted at least six pharma companies* working on coronavirus treatments and vaccines in the U.S., U.K. and South Korea. A few months later, South Korea's intelligence agency claimed that North Korea had attempted to steal information on vaccines and treatments by hacking Pfizer.

Supply chain attacks

As the pharma supply chain becomes increasingly global and complex, cybercriminals are capitalizing on new opportunities.

"One of the approaches we see today is what's referred to as a 'supply chain' attack," says Mann. "In this case, supply chain refers to a 'one to many' attack, where the attack is launched at a third party or a technology manufacturer, but the intent is to reach the companies in its supply chain."

Hackers look for a weak link in cybersecurity protocols and use it as an entry point.

"Cybercriminals attack once, land in many places, and see what can be accomplished. A lot of damage can be done quickly in this manner," says Mann.

The pandemic has further extended the pharma supply chain and by doing so, created more potential points of attack. The

> “ **The thing about cyberthreats is that old experiences fuel new ideas, and the landscape is always changing.** — Liz Mann, EY Americas Life Sciences and Health Cybersecurity leader

need to transport millions of doses of vaccines with unique cold storage requirements has introduced new partners to the pharma supply chain. And these new partners bring new security issues.

A recent BlueVoyant logistics report found that attacks on shipping and logistics firms tripled between 2019 and 2020.[6] While most pharma companies have robust cyber defenses in place, that is not always the case with delivery and logistics companies. Connecting systems via GPS and digital apps exposes all partners in the chain, warns Brill.

As a case in point last November, Americold, the world’s largest owner and operator of temperature-controlled warehouses — and one of the companies tapped to provide the specialized cold storage required for the Pfizer vaccine — disclosed that its computer network was affected by a cyber incident, later revealed to be a ransomware attack.

The attack on Americold wasn’t an isolated incident either. A month later, the cyber teams at IBM and the Department of Homeland Security’s CISA warned of a phishing campaign spanning across six countries that targeted multiple organizations associated with Gavi, The Vaccine Alliance’s Cold Chain Equipment Optimization Platform — a program put in place in 2015 to help improve the global availability and installation of high-performing cold chain equipment.

Insider threats

Insider threats come in various forms, and they don’t always have to be malicious.

As the pandemic took hold, the combination of a hasty transition to remote work, a high-stress climate and the need to work quickly created an environment where even the most well-intentioned employee could inadvertently enable a cyber breach.

In September 2020, cybersecurity experts at Positive Technologies investigated an elaborate social engineering attack against a major pharma company. The attack involved North Korean hackers using a fake LinkedIn profile with hundreds of connections and bogus job offers to trick employees into running code that eventually compromised the corporate network.

There are also occasions where, as the famous line goes, “the call is coming from inside the house.” Aside from occasional data breaches perpetrated by a disgruntled employee, experts at Kroll have spotted a new trend whereby criminals enlist the help of pharma insiders to pull off their attacks.

“In recent weeks, we’ve seen some of the cybercriminal gangs reaching out to people inside an organization and saying, ‘If you will plant some malware for us, we’ll give you a percentage of whatever we get in ransoms,’” says Brill.

To this end, experts have warned of the rise of a new business model used by ransomware developers, referred to as Ransomware as a Service (RaaS). Essentially, criminals are selling kits on the dark web that allow wannabe-hackers who lack the tech skills to develop their own ransomware to simply buy what they need to launch attacks. The ransoms are then shared between the buyer and the RaaS company.

DON’T TURN YOUR BACK

For pharma companies, dealing with cyberthreats is part of doing business. But despite the robustness of systems in place, Brill argues that it must always stay top-of-mind.

“The way I look at it, if you’re in the pharma or biotech business, you may not like to think about it, but you’re in the cyber business,” says Brill. “Whether you like it or not, the risks are there. The only choice is whether you’re going to ignore them or you’re going to understand them.”

As threats change and become more advanced, being proactive has become more crucial.

“What we’ve seen is an evolution in our client base — from ‘protect the perimeter and hope for the best’ to active monitoring, where you really have people looking at what’s going on and trying to get as near to real-time feedback when things go wrong,” says Brill.

Being proactive also extends to situations such as upgrading to new, more connected technologies on the plant floor. The digital plant can offer tremendous benefits, provided manufacturers make cybersecurity part of the discussion from the start.

“The magic lies in recognizing that cybersecurity needs to be embedded in emerging technologies from the outset, and by design,” says Mann. “The mistake organizations make is in introducing new technologies first, and then trying to secure them later. It is better, faster, smarter and less expensive to embed security into the process from the beginning.”

As threats change and become more advanced, being proactive has become more crucial.

Making cybersecurity a top initiative means starting conversations from the top.

Big Pharma has seen the rise of in-house chief information security officer positions and increasingly, according to Mann, these leaders have a seat at the boardroom table. “The movement from the back office/IT to front office/business strategy, is occurring, albeit slowly,” says Mann.

For the smaller companies who may not have the means to have a dedicated cybersecurity executive, there are experts for hire, like Brill and his colleagues working in Kroll’s Global Cyber Risk practice, offering end-to-end cyber-risk solutions. Mann notes that some pharma companies may also opt for a part-time or “on-call” CISO.

“We recognize it’s not always feasible to have a dedicated executive, but the threat is significant, therefore organizations all need to figure out a way to address it,” says Mann.

Brill stresses that cybersecurity can’t happen in a bubble. Recognizing patterns and methods of attack can help defend against breaches. It’s here that experience and exposure makes a big difference.

“We handle several thousand cases a year. And as a result, we’re able to collect a lot of data on what’s happening right now, this week, last week, last month, etc.” says Brill.

Collaboration, or “crowdsourced cyber security” is also a viable method of broadening experience.

The Health Information Sharing and Analysis Center (H-ISAC) is a global, non-profit organization offering health care stakeholders a forum for coordinating and sharing physical and cyberthreat intelligence. The community — which consists of clinicians, payers, pharma, academia and health IT — is focused on sharing intelligence on threats, incidents and vulnerabilities as well as advice and best practices for mitigation.

“As an industry, pharma recognizes that a threat to one is a threat to all,” says Mann. “In my experience, I have seen pharma CISOs help one another during cyberattacks. When human or animal life is at the center of the business, perhaps it inspires better collaboration."

Ultimately, eliminating cyberattacks entirely is not possible, so it comes down to a familiar concept in pharma — managing risk.

"In a nutshell, no one can protect everything with equal rigor. This is a fact. Therefore, risks need to be assessed and defenses implemented based on the likelihood of a breach and the potential for harm," says Mann. "The cyberthreats are significant and ever-changing, so the equation is one of balancing risk with resources." ○

REFERENCES

1. *"2020 Biotech and Pharma Report." November 2020. BlueVoyant.*
2. *"The 2021 Ransomware Risk Pulse: Pharma Manufacturing." 2021. Black Kite.*
3. *"Cyber Espionage, Ransomware and Insider Threats Converge on Pharma and Life Sciences." 2021. Illusive.*
4. *"Cost of a Data Breach Report." 2021. The Ponemon Institute and IBM Security.*
5. *"The State of Incident Response 2021." Kroll, Red Canary, and VMware.*
6. *"Supply Chain Disruptions and Cyber Security in the Logistics Industry." 2021. BlueVoyant*

Slow rush to the cloud

Strategic cloud deployment is critical to achieving business and operational results

By Bob Lenich, Director of Global Life Sciences, Emerson Automation Solutions

From supply chains to the mobile workforce to technology transfer, the pharma industry is figuring out where it makes the most business and operational sense to leverage cloud technologies. Many production systems today can be implemented in the cloud, but there are still very good reasons for keeping some of them on-premise for the foreseeable future.

As organizations consider which systems to move to the cloud and which to keep on-prem, they must consider how to protect both data and process control, while still making it easy to get critical data out of the system to enable enterprise-wide business decisions. Network latency, security and the role of individual systems in business processes should guide any strategy.

A NEW APPROACH

For years, the Purdue Model — an industrial control systems architecture reference model — has been the gold standard for separating enterprise and control system functions into hierarchical zones for improved security and performance. More recently, however, the rapid expansion of IoT devices, along with edge and cloud technologies, has disrupted this hierarchical structure of data flow.

Today, manufacturers rely on data sharing between different levels of the organization and need an architecture to support data flow. The best solutions are tiered —with a mix of local, cloud and hybrid architectures — driven by the needs of plant systems and functions.

Manufacturers rely on data sharing between different levels of the organization and need an architecture to support data flow.

A three-tiered system, consisting of an on-prem control layer, a hybrid real-time production layer, and a cloud-based enterprise layer helps promote successful and secure operations while ensuring data is not trapped in silos, which impede business decisions and technology transfer.

THE ON-PREM CONTROL LAYER

Control components and systems must be fully protected because any incidents occurring at the control level will have the highest impact on safety and production. All components operating at the control layer benefit from low-latency, high-speed and fully redundant networking solutions. Because these are the most mission-critical and time sensitive systems — usually residing on the plant floor — cloud hosting is generally not a reliable or secure enough option. The control layer is typically hosted on-prem to ensure software and equipment have the fastest, most reliable and most secure connections.

Closed-loop process control

Process robotics, machine and equipment control typically reside in the control layer. As the heart of operations for production, the control system always needs a high-speed, low-latency connection to plant equipment and personnel.

Moreover, in continuous control and batch executive operations, many plants use coordination and advanced control strategies, which directly impact lab and production equipment. Continuous operation strategies such as cross-unit coordination drive production processes to a desired state and ensure successful lot production. This cross-unit coordination provides feed-forward and feedback events and triggers, where timing is critical. Keeping the control system in the same physical location as plant equipment ensures network latency or internet outages do not create problems in coordinated responses.

Safety and equipment health

High-speed, low-latency operation is also essential for safety, and for functionality specific to machinery health. The fast network operation available locally at the control layer enables processes and equipment to communicate state changes to trigger interlocks — essential functionality that cannot risk delays from a network outage.

In addition, executing health management functions for critical or hazardous equipment at the control layer enables fast response or trips on machines experiencing faults before they can cause damage or create safety risks.

EASILY MOVING DATA

Nearly all process data flows through the control layer. Even though the control layer will not be hosted in the cloud, organizations still need a method to gather process data, and to pass it securely across the site and enterprise for better business decisions.

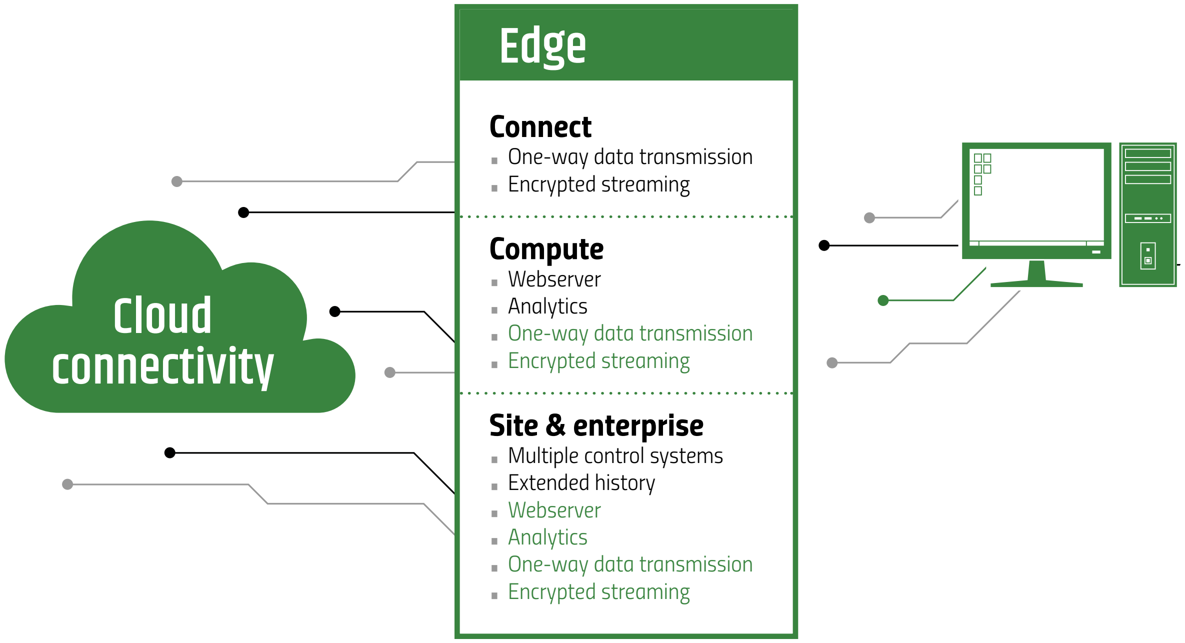
Typically, plants do not want to send control data thousands of miles away to a data center for processing, nor do they want to introduce the security risk of opening the control layer to external internet-connected systems. Edge computing solutions solve this problem by bringing computation and data storage closer to the devices generating data in the control layer.

One key component for implementing edge communication, the edge gateway, provides a solution to securely collect data from the control system, without impacting its performance or uptime (Exhibit 1).

Dedicated security features like one-way data diodes with encrypted messaging can deliver essential data from the plant to enterprise systems without exposing control technologies to the internet. In addition,

EXHIBIT 1

Edge gateways provide a secure way to move data from the control system to the cloud.



Edge

Connect
- One-way data transmission
- Encrypted streaming

Compute
- Webserver
- Analytics
- One-way data transmission
- Encrypted streaming

Site & enterprise
- Multiple control systems
- Extended history
- Webserver
- Analytics
- One-way data transmission
- Encrypted streaming

they remove the need for the complex configuration and the context loss created by sending data to a third-party system such as a historian.

Secure edge gateway configurations function as a one-way IT/OT bridge to pull production data to higher levels of the enterprise. These solutions can also be scaled to support edge analytics, or to contextualize and deliver data from multiple control systems to a hybrid cloud or cloud for enterprise-wide analysis.

THE HYBRID PRODUCTION LAYER

Many pharma production systems rely on real-time data to allow systems and personnel to quickly respond to incidents. These systems perform real-time or near-real-time manufacturing automation and optimization directly impacting production. As a result, they require the security and low latency most easily provided by on-prem technology.

However, real-time production systems also regularly need fast and intuitive connectivity to cloud enterprise systems. These solutions provide access to the corporate-wide material, as well as laboratory and planning information, along with the site-based dashboarding and inventory management necessary to make strategic decisions. Access to these systems must be tightly secured but does not require the low latency of production systems (Exhibit 2). With a hybrid production layer, these systems can be hosted locally on virtual machines to ensure real-time data connectivity, while still providing background cloud connectivity, with front-end interfaces replicating cloud systems.

Manufacturing execution

Many of the real-time systems essential to improved manufacturing execution benefit from stable, low-latency connectivity to plant hardware and systems. In systems like order execution, real-time material management and real-time equipment state management, a delay of even a few seconds can create complications in production, and impact quality or safety.

Today, most production facilities run real-time systems at the production layer to provide low-latency performance, while still making it easy to transfer critical data to enterprise systems in the cloud for more centralized management and performance evaluation.

Continuous monitoring and predictive maintenance

Closed-loop process analytical technology (PAT) and real-time exception (RTE) management also run best on local hardware with access to cloud systems. Like manufacturing execution systems, real-time quality control applications are constantly connected to plant hardware, and they often require real-time alert delivery and response. Plant personnel rely on PAT and RTE systems to deliver critical messages to mobile devices as soon as they occur, enabling staff to respond and intervene before an anomaly impacts production.

In addition, enterprise personnel need the same data — though not in real-time — to track and trend performance of individual production centers across multiple locations. As a result, maintenance and production optimization systems typically perform better in a hybrid environment where they are hosted on local hardware for fast notifications to on-site personnel, but can seamlessly connect and deliver data to cloud systems. Cloud connectivity drives enterprise analytics and predictive modeling — information that is no less critical but far less time sensitive.

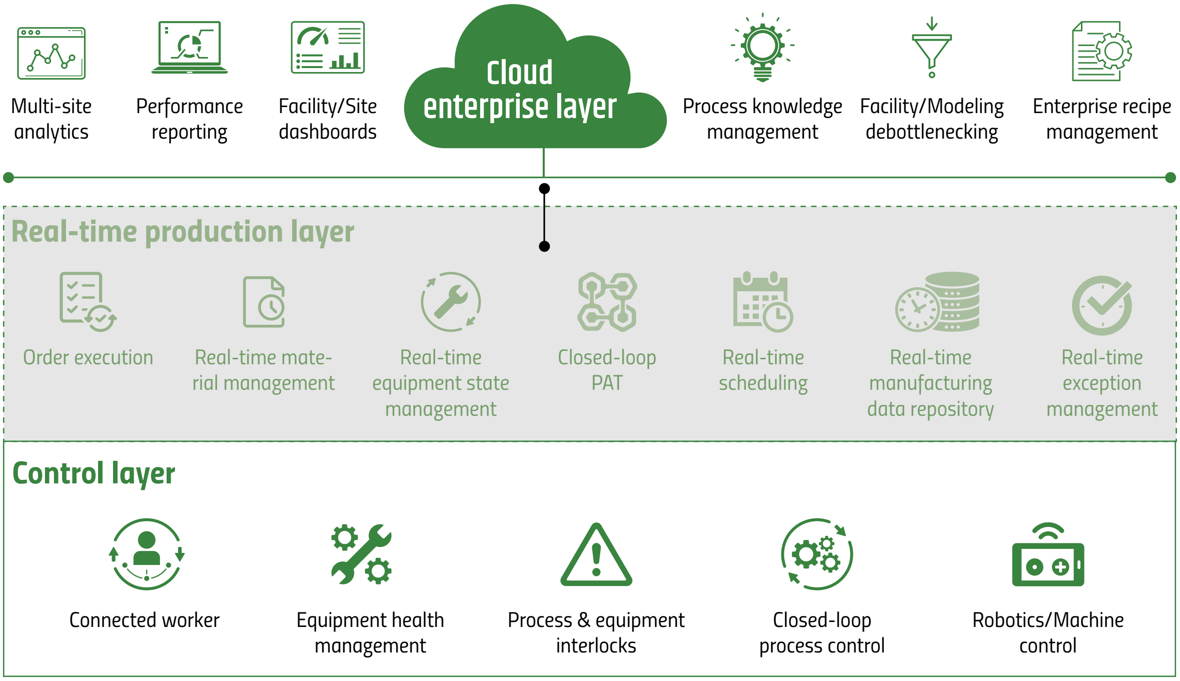
Scheduling

Modern digital scheduling tools offer powerful, real-time scheduling to monitor current production and automatically adjust future production. For high-volume, low-margin plants, this scheduling often necessitates instantaneous status updates, where delays due to network outages or latency cannot be tolerated.

Scheduling software hosted virtually with on-prem equipment offers the best of both worlds, providing the performance necessary to continually update scheduling accurately, while also providing fast cloud

EXHIBIT 2

A three-tiered architecture eliminates data silos while preserving security.


Multi-site analytics
Performance reporting
Facility/Site dashboards
Cloud enterprise layer
Process knowledge management
Facility/Modeling debottlenecking
Enterprise recipe management
Real-time production layer
Order execution
Real-time material management
Real-time equipment state management
Closed-loop PAT
Real-time scheduling
Real-time manufacturing data repository
Real-time exception management
Control layer
Connected worker
Equipment health management
Process & equipment interlocks
Closed-loop process control
Robotics/Machine control

connectivity to schedule data for monitoring, trending and adjustment at the enterprise level.

Data lakes

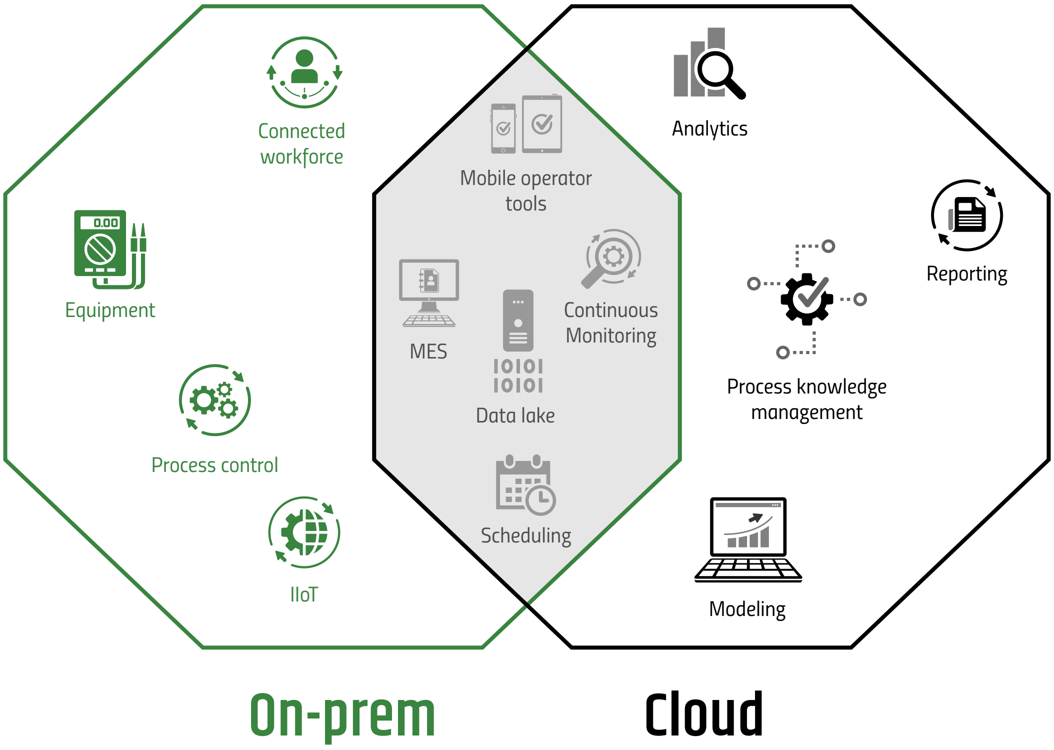
Pharma manufacturers rely on real-time manufacturing data repositories to facilitate easier technology transfer. Research, reliability, operations, maintenance and other departments may all need to collect and use OT data. Data lakes connect the wide variety of software packages used by different departments. They are used to store, standardize and share data in real-time across every stage of a product, from development to production.

Many organizations opt to host data lakes in the cloud. However, other organizations are hesitant to store data in a cloud repository for security and time-sensitivity reasons. These organizations often look to on-prem data lake solutions to improve connectivity and contextualization of data, without relinquishing control of sensitive information.

Such an approach allows organizations far greater control over the data available inside and outside of the corporate network. This ensures continuous access to real-time data without limiting the effectiveness of key enterprise technologies such as advanced analytics, process knowledge

EXHIBIT 3

Knowing which systems should and should not touch the cloud is essential to designing a secure but supportive architecture.



Pharma manufacturers rely on real-time manufacturing data repositories to facilitate easier technology transfer.

management (PKM), and enterprise resource planning (ERP) systems.

THE CLOUD ENTERPRISE LAYER

Enterprise expertise takes a long-term view of operations across time and multiple plants. As a result, data for these tasks does not typically need to be on-site, nor is it heavily reliant on real-time delivery.

Full cloud-based solutions are particularly valuable at the enterprise level, where systems perform less time-sensitive tasks. While cloud systems are highly stable and often boast uptime of higher than 99.9%, scheduled or unscheduled service outages will likely still occur. These outages are more easily tolerated by business-level systems, which are important but won't cause production, safety or quality issues in the event of downtime.

Analytics

Advanced analytics systems use multi-source data coupled with artificial intelligence (AI) and machine learning (ML) to create the powerful predictive technologies enabling speed-to-market.

For analytics systems performing non-real-time multi-site analysis, hardware requirements tend to increase quickly. As a result, investing in on-prem equipment to run models and engines is often cost prohibitive. Cloud systems, however, scale quickly, easily and affordably to keep pace with the needs of complex AI and ML models. Moreover, analytics software in the cloud is regularly updated, ensuring users always have access to the latest and greatest models to drive better production and higher quality.

Cloud hosted applications make it easier to integrate across systems such as performance reporting, facility and site dashboards, ERP and laboratory information management systems. In a growing number of facilities, cloud connectivity continues down to systems in the hybrid space, like electronic lab notebooks and manufacturing execution systems.

Process knowledge and management

PKM applications improve technology transfer and collaboration across the enterprise. These systems thrive in a cloud environment, where anyone in the organization — regardless of location — can quickly access data they need from any stage of therapy development. Process development, material science, technology and other personnel can collaborate to scale recipes and more easily execute technology transfer from anywhere in the world.

Facility modeling and debottlenecking

Manufacturers use modeling and digital twin simulation for a variety of production needs, from testing process changes and eliminating production bottlenecks, to performing predictive maintenance tasks, to training operators to improve performance, quality and safety.

High-fidelity simulations, which start large and continue to grow as new process areas and models are added, are ideal for cloud hosting, where storage and processing power are easily and affordably scalable at a moment's notice (Exhibit 3).

PICKING THE RIGHT ARCHITECTURE

While not all systems need to be hosted on-site, neither is every system ready to run in the cloud. Fortunately, organizations don't need to choose one solution or the other. Instead of rushing to the cloud, organizations should focus on security, performance and safety needs to select an array of architectures supporting equipment and personnel, while maintaining a secure, productive environment.

With the wide range of cloud, hybrid and edge solutions available, it is easy to find the right mix of hosting technologies to improve performance, throughput, and speed to market — while still protecting key elements of development and production such as quality, runtime and security. ○

Pharma's digital prowess put to the test

Positives, negatives and mixed results from this year's Smart Pharma Survey

By Karen Langhauser, Chief Content Director

Pharma Manufacturing's fifth annual Smart Pharma Survey separately asked drug manufacturers and equipment and services vendors* their thoughts on the pharma industry's digital maturity.

While results from our 2019 survey generated concern that the industry's enthusiasm for the digital "revolution" was waning, last year's survey results — fielded six months into the pandemic — were brimming with digital positivity.

With the pandemic persisting, what has become of pharma's digital journey?

As pharma professionals around the globe wait to see what post-pandemic industry will look like (and when it will arrive), this year's mixed bag of survey results reflect that sentiment.

THE POSITIVES

Pharma companies are proactively choosing to automate.

Just over 88% of pharma manufacturers — the highest percentage in survey history — said they believe their company would choose to automate processes if given the option.

*For the purposes of this survey, "vendors" are defined as companies who offer pharma processing equipment, lab equipment, controls or software, as well as contract researching, consulting or related services. There were 36 vendor responses. "Pharma manufacturers" are defined as those who manufacture pharma or biopharma drugs, make APIs or excipients or offer contract manufacturing services. There were 43 manufacturer responses.

For the 5th consecutive year, pharma vendors believe that the No. 1 issue holding back their customers' digital progress is fear of regulatory backlash

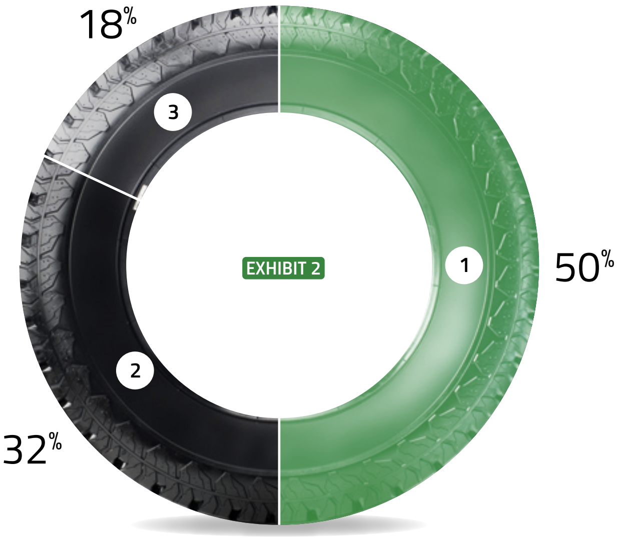
The pandemic has propelled change.
More than half of pharma manufacturers surveyed said that the COVID pandemic has led to more automation and less personnel on the plant floor; increased interest in digitalizing the supply chain and better integrating partners; and an increased use of technology to collect and analyze data in real-time.

THE NEGATIVES

Less than 80% of pharma manufacturers can decisively say the pharma workforce is becoming more comfortable with automation. This is trending way down from last year's 93%.
Are we going backwards, or has it just been a tough year? As companies work through the kinks of rapidly deployed digital solutions, frustration is inevitable.

This year, 27% of equipment vendors claim that when their pharma customers are designing/upgrading their facilities, digitization is "rarely" part of the discussion.
While the majority of pharma manufacturers say digitalization is part of their facility design discussions (Exhibit 4), pharma vendors don't quite agree.

And according to ISPE's Pharma 4.0 Special Interest Group, which has been working since 2015 to translate how Industry 4.0 impacts the pharma industry's unique requirements, this could hold pharma back. ISPE has stated that while smart factory transformations are not a "must," they provide a competitive advantage to the extent that missing out could be a business risk.



Which of the following statements best describes your company's progress on digital transformation/IIoT initiatives?

1. At the starting gate, with focus on learning and exploration
2. We are now identifying early applications to pilot
3. We have identified specific applications and made investments to match

EXHIBIT 3

Top concerns about smart equipment and technology in plants

PHARMA	VENDOR PERCEPTION OF PHARMA
Integration	Integration
Education	Regulatory hurdles
Regulatory hurdles	Big data

WHAT CHANGED

More pharma manufacturers and equipment vendors felt that the responsibility of pushing the drug industry to automate belongs to equipment manufacturers and software providers.

According to survey results, 38% of pharma manufactures and 54% of vendors think that equipment manufacturers and software providers should be proactively leading the charge by offering innovative products and education.

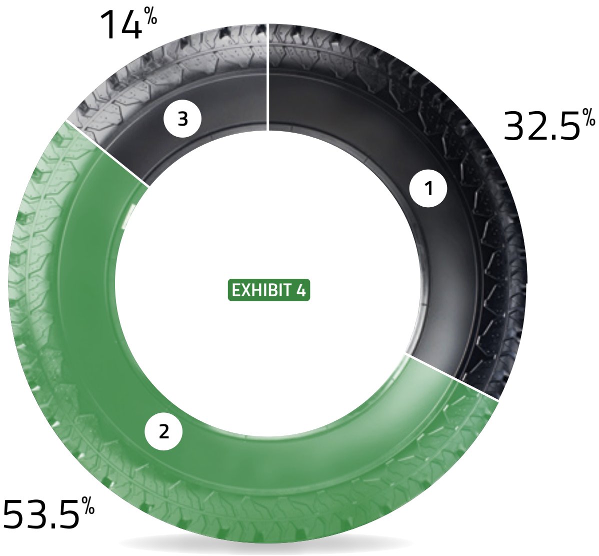
One of the many issues the pandemic has highlighted is the importance of reliable, trusted supply partners. Pharma's core competency is discovering innovative treatments, so an increased reliance of partners to provide the necessary tools could free up the industry to do what it does best.

WHAT STAYED THE SAME

Half of pharma companies are still at the starting gate when it comes to progress on digital transformation/IIoT initiatives.

This finding (Exhibit 2) is consistent with results from the past five years of pharma surveys.

To see how pharma compares on a broader industrial stage, we can look to Smart Industry's most recent State of Initiative report, which compiles results from surveyed professionals from across manufacturing, processing and related industries. When asked about their company's progress on digital transformation initiatives, only about 10% purported to still be at the "starting gate."



When your company is designing or upgrading its manufacturing facilities, how important is digitization to the discussion?

1. It is a leading priority
2. It is important, but not the biggest priority
3. it is rarely part of the discussion

14% of pharma manufacturers say the pandemic hasn't changed the industry's perspective towards digitalization

And yet, the variability in pharma's survey answers can partially be attributed to the lack of a standard, unified method for evaluating a company's digital transformation progress. In short, everyone defines digital success differently.

Pharma's top concerns surrounding smart equipment and technology in plants haven't changed since 2018.

Integrated, defined as, "difficulty integrating new technology with existing lines or equipment" continues to hold the number one spot for both pharma manufacturers and equipment vendors. (Exhibit 3)

This persistent and pervasive hurdle stems from the many legacy systems in operation on the pharma plant floor that lack the capability to connect to high-level automation systems or devices, as well as pharma's need to connect technologies from different suppliers to develop fully integrated processes.

Regulatory hurdles, specifically a lack of regulatory buy-in or understanding of new processes, continue to be cited as an obstacle by both pharma manufacturers and equipment vendors.

This comes in spite of considerable strides made by the U.S. Food and Drug Administration towards shaking the agency's reputation as innovation blockers.

During this year's Parenteral Drug Association annual meeting, Jeffrey Baker, deputy director, Office of Biotechnology Products, Center for Drug Evaluation and Research, challenged the pharma industry's wiliness to modernize in the manufacturing space. According to Baker, although more than 90% of FDA submissions are supplements to Biologics License Applications, very few, if any, reflect modernization or deployment of new manufacturing technologies.

Baker pointed out that despite the fact that regulators are often blamed, the reality is that the FDA has encouraged the development of advanced manufacturing technologies for 20 years through strategic plans, working groups, partnerships and programs.

The pharma industry relies on balancing risk. In the digital sense, this means deciding what risks are worth taking. The most successful digital strategies have often challenged the historical understanding of regulatory policy.

HYGIENIC PUMPS FOR FLUIDS & PASTES: FROM <0,1 ML

- Repeatability of > 99 %
- For one & two component materials
- Gentle handling: Low-shear & pulsation-free
- No dripping due to adjustable suck back
- For low to high viscosity materials
- GMP-compliant hygienic dispensers

Solutions for supplying and dosing or filling of difficult to handle fluids and pastes – for semiautomatic or fully automated packaging lines.

viscotec.com

Addressing gas analysis bottlenecks

New technology allows the end-user to deliver faster, more complete lab quality online gas composition analysis

By Daniel Merriman, Senior Product Manager – Process Analyzers, Environmental and Process Monitoring, Thermo Fisher Scientific

The drug manufacturing process is intricate and nuanced. This can be attributed to health and safety regulations as well as the complexities of the multicomponent mixtures that make up the final product. Processes require constant monitoring, sending test samples to separate labs or input from highly trained staff. The system is plagued by production bottlenecks while workers await test results and can take highly skilled individuals away from R&D and other projects that drive innovation to focus on less productive tasks.

The positive news is that innovation is making headway. Advancements in technology are helping address a specific bottleneck in one of the crucial stages of pharmaceutical manufacturing — gas analysis. New technology available today allows the end-user to deliver faster, more complete, lab quality online gas composition analysis.

BENEFITS OF GAS ANALYSIS

Fluids (water, clean steam and vapor of gas) are a major source of potential contaminants in the pharma manufacturing industry. Some of the gasses used during this process include nitrogen for inerting or flushing, air for flushing, oxygen for fermentation and carbon dioxide for extraction and purification. Monitoring critical process parameters (CPP) with process mass spectrometry gas analysis provides many benefits including:

- Track batch progress in real-time
- Pinpoint contamination and maximize viable cell mass to increase profits

Although it is crucial to monitor gases in the lab, typically a large amount of resources and experts are necessary to conduct this analysis.

- Process mass spectrometer gas analysis benefits
- Reduce over-processing/waste
- Increase product consistency with fault-tolerant operation
- Reliably monitor the composition of gas streams into and out of fermenters and bioreactors

Although it is crucial to monitor gases in the lab, typically a large amount of resources and experts are necessary to conduct this analysis, especially for real-time monitoring of fermentation and cell cultures.

A MORE EFFECTIVE SOLUTION FOR GAS ANALYSIS

Process mass spectrometers are an ideal way to provide continuous analysis of respiratory gases during the manufacturing process. This specific type of device allows the end user to deliver faster, more complete, lab quality online gas composition analysis.

Process gas streams are one of the many analysis methods. A simple analysis of six gases has a 10 second completion time. A more advanced analysis of 40 gases has a 30 second completion time. The user has the ability to select the most efficient peak measurements for each analysis as well as the appropriate speed depending on the process control requirements. The software's stream status keeps the user informed of the analysis.

The speed of mass spectrometry makes it ideal for fermentation and cell culture applications, but speed must not be at the expense of precision. It is equally important that precise data is acquired; otherwise, small changes in concentration will be lost. Over 30 years of industrial experience have shown that magnetic sector analyzers offer the best performance for fermentation off-gas analysis. Key advantages include improved precision, accuracy, long intervals between calibration, and resistance to contamination.

Another key piece of the production process that has received a great deal of attention is the drying process. Gas analysis mass spectrometry has been used extensively on a wide range of dryers, including filter dryers, vacuum dryers, tray dryers, rotary dryers and spray dryers.

UNDERSTANDING THE INNER WORKINGS OF MASS SPECTROMETRY TECHNOLOGY

The primary feature of the process analyzer of the mass spectrometer is the scanning magnetic sector technology.

What is magnetic sector technology? These types of instruments are composed of electric and magnetic fields that bend a beam of ions (any atom or group of atoms that bears one or more positive or negative electrical charges) travelling at relatively high energies. This field-proven technology has demonstrated the highest performance for on-line gas analysis. Scanning magnetic sector technology offers precision, accuracy, long intervals between calibrations, and resistance to contamination.

Another key aspect of the technology is the unique Rapid Multi-Stream (RMS) inlet system (part of newer technology) which allows for the selection of 16 to 64 gas streams and sets new standards for speed and reliability of multi-stream sampling and maintenance intervals. Adopting a RMS system can help manufacturers avoid extra maintenance of multiple instruments.

In an RMS system the position of the rotating arm is optically encoded for reliable computer-controlled stream selection. Downstream of the RMS system is a digital flow sensor to report sample flow for each selected sample point.

The FDA has approved over 20,000 prescription drug products for marketing. With so many different medications on the market, we need reliable and quick ways to enhance the safety of the pharmaceutical manufacturing process and help those making the drugs to meet the high demand. This new gas technology is one key way we can help pharmaceutical manufacturers ensure quality and safety at a quicker pace. Consumers deserve to feel safe when taking their medications and innovations will help us ensure this brand promise. ○

www.PHARMAMANUFACTURING.com
pharma™
MANUFACTURING
THE DRUG INDUSTRY'S VOICE FOR MANUFACTURING EXCELLENCE

ADDITIONAL RESOURCES

EBOOKS

Check out our vast library of information-rich reports that aggregate award-winning content on critical industry topics.

Here

UPCOMING AND ON-DEMAND WEBINARS

A series of live and archived events focused on presenting solutions and strategies to identifiable problems, emerging technologies and key topics that are relevant to today's pharma manufacturing professionals.

Here

PODCAST - OFF-SCRIPT

The Off Script podcast offers in-depth interviews and discussions with industry experts about hot-button topics in pharma, going behind the scenes of Pharma Manufacturing's print and online coverage.

Here

ESSENTIAL REFERENCE GUIDE

Specially designed by the editors of Pharma Manufacturing to provide the most valuable educational content for all pharma manufacturing professionals — from the 20-year veteran to the first-year employee.

Here