# Addressing Pharma's Top Cybersecurity Challenges

Today, pharmaceutical companies face a perfect cybersecurity storm. In an industry already operating in a complex and highly regulated environment, 2020 introduced a massive shift to remote work at the very moment pharma was gearing up to respond to the novel coronavirus and resulting global pandemic. Simultaneously, many pharma organizations were also experiencing the twin forces of consumerization and digital transformation and the demands for ever-increasing agility, responsiveness and transparency.

"Few industries have experienced the same level of disruption as pharma is facing today," said Troy Ament, Healthcare Field CISO for Fortinet, a multinational cybersecurity provider serving 48,000 clients from its headquarters in Sunnyvale, California. "When you begin with large, highly complex and highly innovative companies that span national borders, it's already going to be a challenge to manage the security, technology and people who support critical business outcomes. But when you add in the underlying structural transformation that pharma is experiencing – and a global pandemic on top of that – cybersecurity threats multiply very quickly."

## Layers of complexity

Ament was one of two featured speakers at a November 2020 virtual deep dive into pharma's top cybersecurity challenges. His co-presenter, Simon Roach, the former CIO of Global Pharmaceuticals for GSK and who now serves as a security consultant, echoed Ament's observations. He noted that the same characteristics that make pharma so dynamic also introduce industry-specific risks that keep CIOs and CISOs up at night.

"Pharma brings together a very, very diverse set of disciplines – biology, chemistry, genetics, physics, manufacturing, distribution – and a whole range of technical capabilities in shifting collaborations to create an asset, medicine, which has a limited lifespan in terms of intellectual property that can be commercialized," Roach said. "So you *begin* with massive network complexity, which is the first challenge from a security and control perspective."

In addition to complexity, Roach said three other characteristics of the pharmaceutical industry complicate the information security posture of leading organizations: heterogeneity, agility and culture.

*"Easily one of the biggest obstacles to supporting cybersecurity maturity within an organization is being able to support digital transformation. There are many components to this – connected medical devices, connected OT devices and cloud migrations – and it is all happening at once."*

**Troy Ament** | Healthcare Field CISO | Fortinet

*Heterogeneity* refers to the process of IT complexity due to mergers, acquisitions and divestments. Often, legacy IT assets remain operationally functional, but they have surpassed their cybersecurity lifecycle and are difficult, if not impossible, to secure against quickly evolving threats.

"Think about the way the pharma companies have grown up over many years," Roach said. "Some of them are hundreds of years old and they've been born out of lots of acquisitions, mergers, divestments of different assets, etc. So, you end up with quite a diverse set of technologies that are harnessed by that company to do business."

The next characteristic is *agility*, Roach said. In the race to develop a new medicine, speed is essential, so organizations try to minimize the boundaries and obstacles between research, development and commercialization.

"From the perspective of experimentation in the labs through to scaling up manufacturing pilot plants through to commercial manufacture, you have this combination of aging and complex IT and operational technology [OT]," Roach said. "That represents a significant risk to manage, as well."

The final characteristic is *culture*. On the one hand, scientific advances require a culture of data sharing and openness, Roach explained. But on the other hand, pharma "IP is locked up in that very same information, so they need to secure it, to lock it down. That's a major dilemma."

## Digital transformation presents challenges

Newer developments are raising both the stakes and the challenges for pharma cybersecurity, but perhaps none so much as digital transformation according to Ament.

"Easily one of the biggest obstacles to supporting cybersecurity maturity within an organization is being able to support digital transformation," he said. "There are many components to this – connected medical devices, connected OT devices and cloud migrations – and it is all happening at once."

It's incredibly difficult, Roach agreed, "when you've got that heavy compliance and regulatory burden, and you've got a conservative attitude towards risk. Then, the adoption of newer technologies and digital transformation becomes challenging."

Roach said pharma "was late to the game" but is now poised to embrace digital transformation because of the substantial benefits it offers. Moving critical data into the cloud, for instance, may create new security concerns, but the ability to spin up instances and quickly provision new workspaces, slice and dice data to foster greater collaboration with partners and expand compute and storage capabilities with the push of a button provides pharma organizations a significant reduction in infrastructure's total cost of ownership.

Although the COVID-19 pandemic has validated the cloud-based approach, Ament said, it has also highlighted its vulnerabilities. "Like every other industry, pharma had to respond immediately and shift to a remote workforce," he contended. "But telework creates a huge number of new endpoints outside the traditional network – new blind spots – that need to be secured."

And that's not merely a technology challenge, Roach observed. Already a persistent concern for pharma CISOs, insider threats – both intentional and accidental – have been multiplied by the unplanned shift to remote workforces.

"In a traditional environment, even though you've got many different partners and collaborations developing intellectual property, you do that within the walls of a laboratory, a research facility or a commercial organization," he said. "You've got a whole range of physical and behavioral controls that exist around the people that operate in that arena. But as soon as you take those people out of that environment where they're working remotely, then you lose all of that physical and behavioral oversight."

Digital transformation is also driving pharma to extend data connections directly to patients. More and more organizations collect data from clinical trials from participants using mobile phones, tablets, wearables and other internet of things (IOT) devices, Ament noted. While that removes much of the friction for patients, it places an increased burden on the organization to ensure the security and integrity of data arriving from endpoints over which the CISO may have little or no control.

*"I've seen examples where there was extensive use of malware detection software, and yet, a ransomware threat succeeded because the virus definition wasn't current enough to recognize it. In those situations, it becomes incredibly important that you have a great backup regime, good disaster recovery approaches, and test those regularly."*

**Simon Roach** | Former CIO of Global Pharmaceuticals R&D for GSK | Security Consultant

## The best defense – a good offense

Both Ament and Roach contend that the greatest threat now facing pharma is the same one stalking other industries – ransomware.

"The increasing sophistication of ransomware attacks, combined with the added risks of teleworking, really amplifies both the risks and consequences of a successful exploit," Roach said. "I've seen examples where there was extensive use of malware detection software, and yet, a ransomware threat succeeded because the virus definition wasn't current enough to recognize it. In those situations, it becomes incredibly important that you have a great backup regime, good disaster recovery approaches, and test those regularly."

According to Ament, the most successful pharma organizations take a foundational approach to cybersecurity. This approach features an enterprisewide understanding – from rank-and-file workers to C-suite executives and board directors – of the importance of cybersecurity and stresses governance, risk assessments, data resilience, redundancy and employee training.

"In my experience, the best-prepared organizations embed a high level of governance and good planning into acquisitions," he said. "Companies that don't have a governance model that really bakes security into their overall structure and business plan often fail to grow – or will slow down – because their organization becomes too complex to operate efficiently."

Roach said the complexity of the organizational challenges, combined with the severity of threats from malicious actors, is likely to drive new partnerships with cybersecurity vendors.

"The final challenge for pharmaceutical companies is getting the right talent to address these risks," he argued. "The ones that are successful recognize they can't grow all of that talent inside the organization. And the secret to accessing that knowledge and talent is to partner with the companies, corporations or organizations that have the expertise to solve your problems."

*"The best-prepared organizations embed a high level of governance and good planning into acquisitions. Companies that don't have a governance model that really bakes security into their overall structure and business plan often fail to grow – or will slow down – because their organization becomes too complex to operate efficiently."*

**Troy Ament**

**To learn more about cybersecurity best practices for pharmaceutical organizations, visit fortinet.com/solutions/pharma.**



Produced by HIMSS | www.himss.org | ©2020