NORTHWAVE
CYBER SECURITY

From crippling crisis to continuous control

NextPharma's journey to Cyber Resilience and NIS2 readiness.

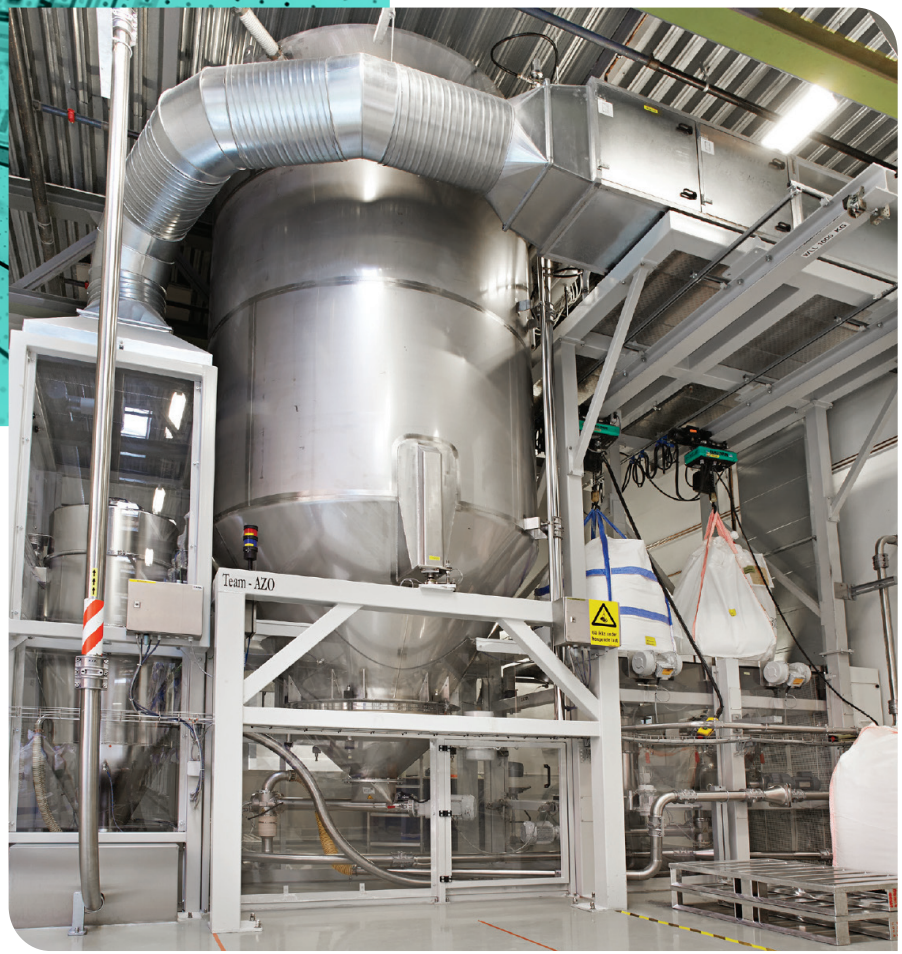
On a rainy September night in 2019, the phone rang at the Northwave Computer Emergency Alarm Center. On the other end of the line was the CFO of Nextpharma, a German based pharmaceutical company. He was asking the team for help with what was soon determined to be a ransomware attack. Criminals had succeeded in encrypting business critical IT systems throughout multiple networks, bringing the company to a standstill…

More than four years later, we are speaking with NextPharma's CIO, Joel Fidalgo, who has joined the company in 2022 and since then overseen the company's journey in cyber resilience and digitisation.

Joel Fidalgo
Is NextPharma's CIO since 2022

NextPharma

"We are a leading pharmaceutical CDMO (Contract & Development Manufacturing Organisation) in the European Union, and we produce all kind of different medicines for our customers and ultimately the patients around the world. Our customers choose us and possibly us over others and trust us with the manufacture of their products. This means that the continuity of delivering medicines to the patient, is our key focus. So, any risk that could disrupt our operations and capability to deliver our products has my full attention. Next to this, the integrity of our production and laboratory processes is key. We are under strict rules and responsible for delivering a working medicine to patients. This means that all the production processes have to be secured and validated. We must proof the integrity of the production process, before we can release the drug to the patient. On top of that, we also have our R&D, trade secrets and intellectual property of our customers to protect. We invest heavily in capacity, efficiencies, and innovations, and we need to see the financial results from those investments by continuation of delivering high quality products to our customers. And finally, there is compliance. I think there is a necessity of compliance to regulations as such, but to me this is hardly an issue because the way we manage our cyber security and other IT processes almost 'automatically' leads to compliance, because we are following good industry practices and standards."



"Doing M&A means increasing your risk dynamics."

Nextpharma is headquartered in the United Kingdom and operates factories in Finland, France, Germany, Norway, and Scotland.

Nextpharma operates from multiple locations in Europe. There is high diversity in in the way that sites are structured, and each company subsidiary is dealing with unique legacy topics on production- or laboratory machinery. Their ongoing M&A activities increase the dynamics and complexity of their cyber risk as the company continues to grow. **We ask Joel how he deals with this.**

"I think for me always important is to objectively understand the current situation and work from there. In essence we follow a PDCA cycle, although we are not ISO27001 certified. Our growth strategy creates dynamics in our risk. Every company that we acquire has a different starting point, a different complexity to deal with. So, it is always important to understand where we are and make a plan with prioritisation. Our approach from the beginning was to focus on ensuring core fundamental basic security hygiene first and deploy your Managed Detection & Response and SOC services, to create a permanent watch over our infrastructure and feed us insights into how we are doing. To this day, this is still for me one of the best investments in our security, as it so often helped earlier identifying potential risks and threats. Later on, we focused on the processes and the human behavioral side. We keep doing this, working from objective understanding on where we stand and then continuously improving."

This is also the approach for each site we did integrate during our journey and might integrate in future.

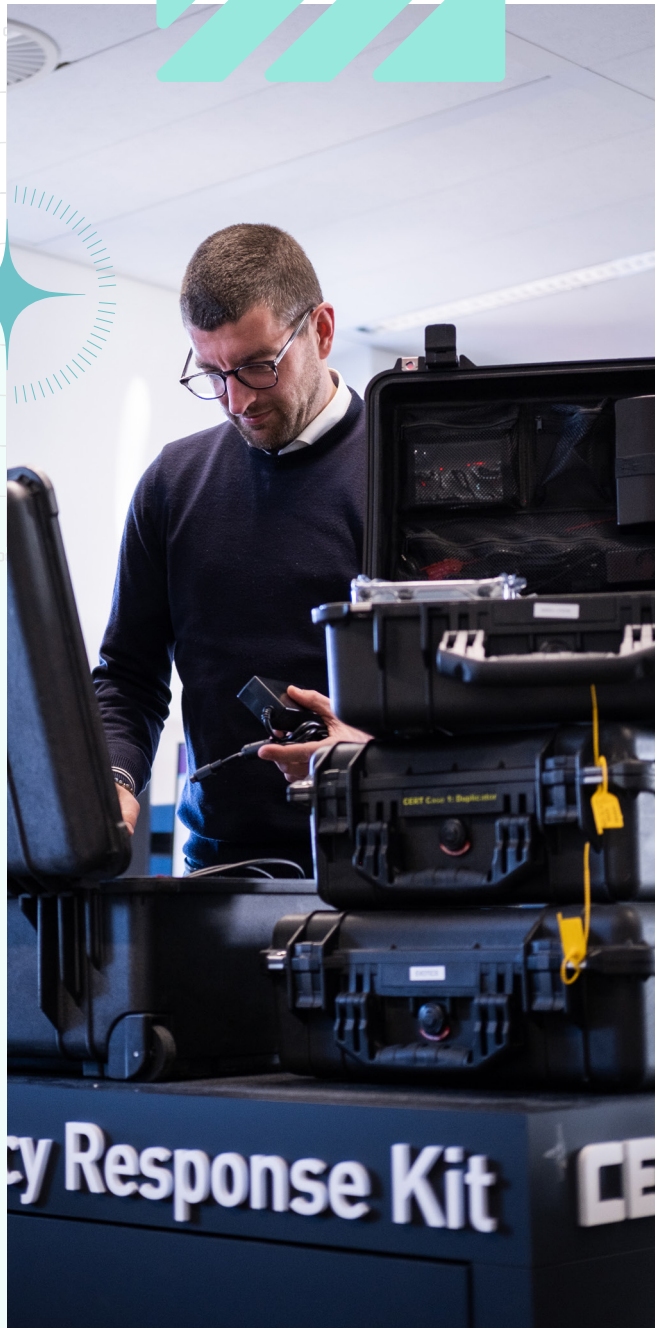
The concern around supply chain security is one that is not exclusive to Nextpharma. In a survey on the NIS2 directive that we did among 50 CFOs of midsize and large industrial enterprises, we discovered that almost all of them mark supply chain risks management as the single biggest challenge they see. **Is this a problem for Joel as well?**

For NextPharma, the threat landscape changes rapidly and aggressively, with increasing number of state actors interested in intellectual property and more complex cybercriminal attacks. **How does Joel keep track of all these developments?**

"For us it is too difficult to keep oversight of all those variations. You guys are helping us to focus on the right threats and help identify the risks levels. I mean there's a lot of things we do internally to understand what is important for us, what do we need to protect. However, keeping an eye on what happens out there is difficult. Also, the move into more supply chain related attacks is a different level of complexity that is very difficult to handle only by ourselves, given our team size. We concentrate on our most important resources in close co-operation with our partners focussing on what is going on in the world to ensure smooth operational security.

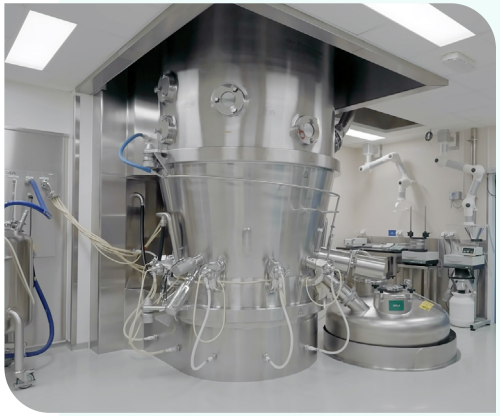
"It would be nice if supply chain risk management would become less of a headache."

"For me there's two aspects on the supply chain issue. The "more simple" one is about third-party solutions on the technology side. That means, we work with partners who are certified and are regularly tested; quite straightforward, as the number is manageable and we are able to act quickly in the event of incidents in this supply chain. It is not so "easy" when it comes to assessing the supply chain of our various materials and other suppliers in our supply chain. Like in many other industries also in the pharma industry, a lot of these materials are coming from various different countries with different regulations around the world. It's very difficult to assess the security level for all of those suppliers. Of course, we take a risk-based approach and focus on the high-risk calibers and use questionnaires to gage their maturity. But it's all very inefficient. Don't forget, we are also in the middle of many supply chains, so that we, on our part are also repeatedly evaluated by our customers and supervisory authorities. It would be nice if some sort of standard is developed, so this supply chain management can be less of a headache. I see this in other industries, but so far, our own industry is unfortunately not there yet."



“Realising resilience is all about creating confidence.”

Although regulations forcing companies to gain control over their security posture are far from new, the NIS2 directive is drawing a lot of attention. The directive aims to improve cyber resilience and Nextpharma has aligned its approach to this directive, even though the directive has not yet been implemented and there is no formal need to comply. **We ask Joel why he is in such a hurry.**



“I think overall NIS2 will be an important driver to improving cyber resilience, especially for less mature companies. We are a leading company in our industry, why for me it is also clear that I would like to lead here as well to be ahead of the curve and not be surprised afterwards. For us it was a great opportunity to review our current state, so we did an exercise and gap workshop to base our improvements on. We were lacking on the process side, where we, as a fast-growing company must adopt better processes to ensure that we keep robustness in how our people behave and perform around an incident. I think the key awareness is that whatever you do, it will someday show not to be enough. This is something to be accepted. So, you need to ask yourself: How can we recover from that situation? We will continue to challenge ourselves with accurate simulations. How could an attacker attack us? How would they think? Realistic adversary simulations incorporated in crisis management exercises. It is also important to show to our customers that we are confident about our cyber resilience. That’s what you want to do as well.”

Joel’s journey over the past four years has brought Nextpharma from a crippling crisis to a situation where the company is now in continuous control of their cyber security and is structurally adjusting its resilience to the company’s growth as well as the latest threats. With compliancy to key cyber regulations as a ‘natural’ outcome. **How does he look back on these four years and what are his key insights for others wanting to make this journey?**

“I think the key lies in always objectively understanding where you are. Either you can create this perspective on your own or you need help to understand where you are and be objective about this, not emotional. For me it was easy in the beginning. I was new to the company, so I was therefore able to objectively assess where the company stood. But in general, I think this objectiveness needs an external and independent as well experienced pair of eyes. Understand your actual risk, prioritise from there and repeat that cycle. We have made very good progress in doing this. At the same time, it still took a couple of years to get to where we are today. We have been lucky that we didn’t suffer a successful cyber-attack during that time. I think what we should have done differently, is to also have more focus on preparing for that imminent scenario of being breached. Simultaneously to all the improvements that we were making. I am sure that the team would have been even more confident, and I believe that is what resilience is all about.”

Would you like us to assist you on your journey towards cyber resilience and NIS2 readiness? You can reach us at:

NORTHWAVE
CYBER SECURITY

E: info@northwave-cybersecurity.com
T: +31 (0) 30 303 1240
W: northwave-cybersecurity.com