A case study with material solely for discussion. Aquantos is a fictional organisation along with the names of the executives. The case does not illustrate effective or ineffective handling of a managerial situation.

AQUANTOS

The Senior Leadership Team (SLT) of Aquantos were busy preparing for the quarterly board meeting, putting their finishing touches to key presentations, memorising data and rehearsing arguments. Although the company was on track for yet another record-breaking quarter following the two previous ones, the quiet satisfaction of jobs well done and exceptional financial performance was tempered by the ongoing challenges of the COVID 19 pandemic and, more importantly, the approach three weeks ago by a competitor proposing a merger.

Each member of the SLT was under no illusion that behind the offer of a merger was the threat of a potential takeover if merger talks made no progress. A deal book had already been put together and it was expected that this board meeting would be focussed mainly on developing the analysis and strategy for negotiations.

Aquantos is a top five, full-service, clinical research organization (CRO). Founded in 1990 by Dr John Saker PhD, Aquantos has 30 years of experience in supporting clinical trials and regulatory submissions for pharmaceutical, biotechnology, and medical device companies. The firm offers comprehensive clinical development services, including biostatistics, statistical programming, medical writing, clinical monitoring, project management and data management, for a single study or an entire clinical program.

In the last 15 years, the company expanded its service offering to preparation of integrated summary documents and CDISC data for regulatory filings in a few different jurisdictions across the Americas, Europe and recently the far East. Effectively becoming a one-stop shop for outsourced trials and submission. The firm built a strong reputation for scientific integrity in its service delivery and developed strong relationships with a wide range of biotech and pharmaceutical companies. The company's own marketing literature states that, due to its "unwavering commitment to scientific integrity, client focus and exceptional performance, long-lasting client relationships are the firm's hallmark."

Over the last 5 years the company's focus on novel drug development led to success when handling the unknowns that arise across complicated therapeutic areas, such as rare/ultra-rare disease, advanced therapies, oncology, and infectious disease trials. This built the firm's reputation as the go-to CRO for complex or novel solutions that were scientifically rigorous. At the start of the pandemic, during the rush to develop COVID vaccines, Aquantos was actively involved with several key pharma firms across Europe and the US in developing robust accelerated clinical trials programs. With government money no object, Aquantos rode the coattails of exceptional financial performance by its key clients.

The firm reached a milestone of 15,000 employees 6 months ago, with operations in the US, Canada, Mexico, France, Germany, Austria, UK, Ireland, Japan, South Korea, Ukraine and Russia. Last year a sales office had been opened in Hong Kong with the plan of opening an operation on the mainland in the following year. Until the start of the Pandemic, Aquantos had seen steady growth and an above average return to shareholders. As a result, the stock market and analysts had been kind to the firm, and it enjoyed a healthy share price with its shares reasonably well traded for the sector. Investors included individuals, corporates, and some funds. The company's own employees were also able to take advantage of a generous stock ownership plan.

Management and Governance

Aquantos's management team was weighted more towards technical expertise than is normal in CROs. The SLT consisted of the CEO, John Troos PhD, and his seven direct reports: Lucy Grey, CFO and Chief Risk Officer (CRO); James Blunt, Chief Marketing Officer; Dan Moorhouse, senior vice -president responsible for all operations (COO), Damian Teylor, chief human resources officer; Dr Joyce Sims PhD, vice-president, regulatory affairs; Dr Jackie Chan PhD, the chief scientist and vice-president R&D; and Phil Stiles as head of legal and corporate secretary.

Two executives reported to Lucy Grey (CRO): Dave Bibble, the chief information officer (CIO), and Pat Butler, the company's chief information security officer (CISO). Three regional / divisional vice-presidents reported to Moorhouse.

The SLT was clearly a well-functioning high performing team and used to having robust, healthy, challenging conversations. Butler joined the team most recently as CISO 18 months ago, as the CEO increasingly realised that they needed to better protect their data assets. In this new role he was to develop new policies, crisis management plans, procedures, and protections specifically to mitigate against cyber risks.

The firm also has 7 non-executive directors on its board, including the CEO. The Chair was the founding CEO, Dr John Saker PhD. The other 6 were all independent and had a good mix of industry experience.

There were four committees that met regularly: audit, risk, governance, and human resources. Each committee was chaired by an independent director and had three other members.

Information Management and Security

By necessity, Aquantos stored a huge amount of data. The usual data found in all corporates plus a large amount of highly sensitive and personal health information about patients, and information about customers drug trials, drug patents and other highly sensitive, confidential data.

Aquantos considered its IT infrastructure to be up to date and secure. There were encrypted backups for all data in 3 different locations and the company and data storage facilities followed the NIST Cybersecurity Framework.
Butler the new CISO had also created several policies and procedures in his first year on the job and he was also tasked to make regular reports to the executive team and the board. The first such report was on the agenda for the upcoming board meeting (Exhibit 1).

Aquantos had not experienced a cyber-attack so far but was ready for the eventuality with draft business continuity, incident response and disaster recovery plans. Butler had not yet managed to create a cyber-breach response plan (play book) across all risk, but he had this on his work plan for the coming year, along with testing of the response plans.

The Proposed Merger

The Chair of one of Aquantos's competitors, a company of similar size, operating in mostly the same markets and with a similar scientifically rigorous ethos, but with complimentary services, approached the Aquantos Chair with the proposal of merging the two companies.

She suggested that the companies were more co-operators than competitors, emphasising the suite of complimentary services and differing client base. The competitor's Chair also claimed that whilst the two companies were in similar geographical markets, her company had expanded into some specific markets that Aquantos was not yet operating in. In sum, merging the two companies would present a great opportunity for long-term, sustainable value creation for the shareholders. A bigger and stronger company could emerge, and significant cost reductions would also be made possible by eliminating the duplication of certain functions and internal services.

Because both firms' share prices and market caps were roughly the same, the argument was that a merger made the most sense. This would avoid what would likely become a long, protracted, and expensive takeover. Both Chairs knew that most such acquisitions failed, and even when they succeeded, it was at a significant cost.

The Aquantos Chair had reported the contact to the CEO, as was his duty. Troos expressed cautious interest in the deal and instructed Grey, the CFO, to assemble a deal team, retain M&A advisors, and begin conducting a preliminary investigation into the merger. They shared all of this with the board in a conference call, warning the directors to keep it confidential and communicate only with him, the Chair or the CFO.

The internal team had spent the last two weeks on the project, assessing the pros and cons of the deal. The team would be presenting its findings to the board at the upcoming meeting with the recommendation to proceed with the merger and enter preliminary negotiations with the competitor. Aquantos's directors were not unanimous in supporting the merger but were keeping an open mind.

As expected, the Board spent minimum time on housekeeping matters and focussed on discussing the merger proposal. The analysis presented by the head of the deal team was well received. The merger's structure looked favourable and promised to create considerable value through both opportunities for market expansion, and cost reductions from eliminating duplicate efforts and departments. The deal team had recommended proceeding to the due diligence stage of the merger.

Ransomware Attack

Before the board could vote on the proceedings, Lucy Grey, the CFO/CRO, looked up from her phone and the urgent message she had just received. She interrupted the meeting to report that the message was from Pat Butler, the CISO. He had just discovered that Aquantos had been the victim of a ransomware attack earlier in the day. Specifically, the ransomware had encrypted Aquantos's customer database with a code that required a key only possessed by whoever had unleashed the ransomware. As a result, Aquantos could not process or bill any orders.

Grey stated further that Butler had not been able to recover the files from the company's numerous on and off-site backups. The files had likely been infected during a waiting period, the delay created by the hackers to allow time for the ransomware to infiltrate all the backups through the normal backup procedures. Most of the files had been encrypted as a result, and those that had not, failed to open because of hardware failures or other technical difficulties.

Ransomware was a particularly malicious piece of code – malware designed to cause a disruption or damage – that usually infected a company's information system when someone within the company inadvertently opened a suspicious attachment from an email or text. The code in question would encrypt the infected system's files. Encryption was usually followed by an email from the perpetrator demanding a ransom to release the key that would decrypt the files. This ransom was usually paid using Bitcoin or another cryptocurrency.

The problems with ransomware attacks were twofold. Firstly, it was virtually impossible to decrypt the files that had been encrypted. Hackers used the same level of encryption used by banks and credit card companies. Second and more disturbing was that about half the time, companies could also not recover files from backups, either because they did not work when accessed or because the backup files had been encrypted in turn.

From recent research that Grey had read, she knew that ransomware attacks were frequent events, with criminals launching over 10,000 attacks daily across the world. The attacks constituted fraud and were reportable crimes (federal in the US), although not all companies disclosed the event. Based on known incidents, up to 60% of companies had reported being attacked by ransomware in the past year, with most of them quietly paying a ransom. Ransoms ranged from $10,000 - $50,000, with more valuable encryptions sometimes getting ransoms well into the six figures. Paying the ransom was no guarantee, however. Companies reported that they had been able to retrieve encrypted files after paying the ransom only 75% of the time. In 25% of the cases, decryption keys were either not provided by the criminals or did not work.

Grey reported that Butler had contacted Aquantos's cybersecurity provider, and they were busy repairing the flaw that allowed the malware through. Future successful attacks were thought to be unlikely.

Grey stated that the hackers had demanded a ransom of $25,000. She recommended to the board that it be paid.

As the CEO, what should you do?

To structure your thinking:

1. **Is this a crisis yet? Should you step away from the board meeting? Who else should you involve in your thinking and decision making?**

2. **Should you pay the ransom?**

3. **Because of your decision (to pay or not) are there any other actions you need to take to ensure that the spread of the attack is stopped, vulnerabilities are closed, and systems and data are recovered safely and securely?**

4. **Is there anything else you should be thinking about? Or doing?**

APPENDIX 1: The rise of the CRO – PharmaTimes Magazine, March 2019. Abridged for inclusion

Around the time he was helping draft the US constitution Benjamin Franklin produced an adage that many corporate investors live by to this day: "Be studious in your profession, and you will be learned. Be industrious and frugal, and you will succeed."

The growth of contract research organisations (CROs) in biopharma seemed to mirror this outlook. CROs flourish because the business case for taking elements of drug discovery out of house and contracting with dedicated specialists has demonstrated itself to be sound. The notion of an industrious collaborator that allows an organisation to maintain the sharpest possible focus on innovation has delivered efficiency gains and helped the industry adopt a more measured approach to overheads.

The restructuring in the pharma industry over the last decade has doubtless helped drive the growth of the CROs, but it's important not to see this trend in isolation. Globalisation and technological advances are part of a bigger wave that pushes all industries, regardless of sector, to be lean and find new ways of working. Contracting out has long been commonplace in the automotive sector, for example, and in the reshaped world of pharma, commercial collaborations have gained credibility and traction.

The success of CROs has come to be regarded as good medicine for pharma, and, in turn, continues to prompt deals that consolidate key players within the different levels of the sector. M&A activity has moved the highly fragmented CRO marketplace to one with a handful of giants and a middle ground where a new generation of significant participants is making its presence felt. At the entry level, meanwhile, there's a myriad of specialists operating across a broad spectrum of services and therapeutic areas.

Five CROs now hold over 33% of the global market, led by Laboratory Corporation of America Holdings (Covance).

Another part of the consolidation/growth mix is CROs looking for a broad geographical footprint. Essentially, they want closer proximity to potential customers – valuable when working on complex/technical projects where client collaboration is key. The influence of smart software is also making its presence felt, with companies such as Medchemica exploring the use of artificial intelligence in medicinal chemistry.

For the broader-based CROs, the big picture aspiration is typically to reach the dimension of an organisation like PPD. Since being founded in North Carolina in 1985, PPD has grown to operate in 48 different countries and has 21,000 staff. The company provides a comprehensive range of services – including integrated drug development, laboratory and life-cycle management. Its clients and partners show the breadth of the market, encompassing pharmaceutical, biotechnology, medical device, and academic and government organisations.

By gaining scale, CROs are able to broaden their propositions to a more integrated offering to meet demand at the top end of industry. Big pharma generally wants to outsource larger packages to fewer people – not least because it makes it easier to manage. But there has also been marked growth across a spectrum of specialist CROs, delivering work for small and mid-sized biotechs.

A decade ago, CROs were generally only considered for clinical trials and lab services. These days the market has evolved to cover data and analytics for trial insights and design, drug development planning, medical affairs and regulatory consulting. Growth has also come from rising demand for safety and pharmacovigilance, clinical trial feasibility and protocol optimisation.

By therapeutic area the CRO market can be divided into segments that include cancer, infectious diseases, central nervous system disorders, cardiovascular diseases and other therapeutic areas, which include diabetes and various metabolic, dermatology and respiratory diseases.

The market can also be considered in relation to the type of service the CROs are providing and where they fit in the drug development phases. The biggest and overarching category is simply drug discovery but there are many specialist CROs concentrating on areas such as preclinical studies to determine relative toxicity, Phase I to test basic safety and pharmacology, Phase II efficacy evaluation and Phase III advanced efficacy and safety testing to provide enough data for valid statistical conclusions required by the regulatory authority. Finally, there's Phase IV continuous testing following marketing approval.

Other more general CRO services including pharmacovigilance, bio-statistics, clinical data management, site management, monitoring, regulatory services, protocol development, and medical writing have done well. In the North West, medical communications has also grown in tandem with the rise of CROs, and is adding to a regional cluster of providers such as Ashfield Communications and newer entrants, including Helios, Spirit Medical and Bioscript.

The dynamism in the CRO market is not going away and the next wave of expansion could well see CROs either merge with or acquire data companies. Technologies have a way of converging and the alignment of big data and using it to streamline clinical developments is an intriguing possibility. The relentless rise of information technology and digital health has deep implications for clinical trials, for example.

The need to make data-driven decisions and elevate the quality of trials by leveraging technology is already making its presence felt and CROs are becoming part of the solution. Data mining of complex trial data is now a service area. The days of one or two endpoints are passing, there's now a much wider area of complex data explored.

CROs can thrive, operating in an environment where they have easy access to a large pool of potential collaborators and customers all focused on the same imperative: growth.

A case study with material solely for discussion. Aquantos is a fictional organisation along with the names of the executives. The case does not illustrate effective or ineffective handling of a managerial situation.

Exhibit 1: Aquantos Board Cyber Report

1 of 2

1. External Cyber Incidents

1. According to industry reports there has been a 50% increase in reported phishing campaigns aimed at Pharmaceutical companies. There have been 9 such campaigns reported in the last quarter.

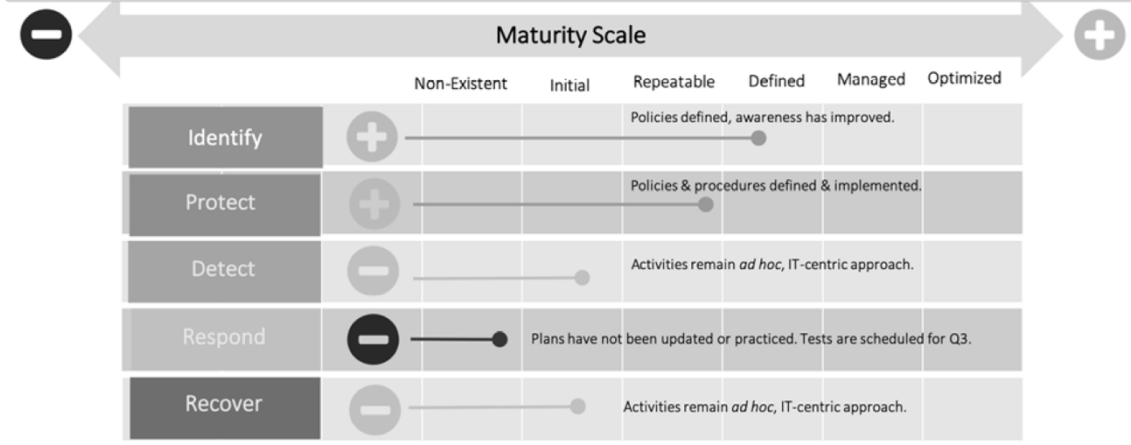
2. Internal Cyber Incidents

1. There were 25 phishing campaigns aimed at members of the Executive Team, with no business impact.
2. There were 9 phishing campaigns aimed at IP assets, with no business impact. .

3. Narrative

- Industry phishing metrics have increased by 50% & internal phishing campaigns by 300%.
- Cyber teams are puzzled – and are investigating what is the potential root cause and why internal numbers are higher.
- Currently no business impact. We plan to monitor more closely and adjust Operations as necessary, reporting back as needed.
- Upcoming cyber exercises in Q3 and Q4:
  - Red /Blue Team exercise
  - 3rd-party Penetration testing
  - Enterprise Phishing training campaign and test.

2 of 2



*Note: The scorecard is based on the NIST Cyber Security Framework.

Source: Company files.