Cyber Attack on XYZ Biotech

Background

XYZ Biotech is a 15 year old life sciences company focused on developing biologics for treating brain diseases. It went public 5 years ago as it was releasing its first product that has been very successful in treating a niche neurological disorder. However, the real market interest is a result of its pipeline which is dominated by compounds that are expected to provide significant results against Parkinson's and Alzheimer's disease.

In particular, XYZ's Parkinson's disease is well along in its Phase III Clinical Trial with approval by the FDA expected within six months. The market is aware of, and excited by, this progress and XYZ's stock has risen by 40% within the last six weeks.

The Incident

A criminal group of cyber attackers has penetrated XYZ's defenses and exfiltrated significant portions of both its clinical trial data base and the associated patient data base. The attackers have contacted the company and demanded a $5M payment via Bitcoin within the next two weeks or they will launch a campaign to threaten the Parkinson's disease clinical trial. In an initial review of its systems, XYZ Biotech was not able to confirm the penetration and there have been unconfirmed rumors in the industry about attempts to shakedown companies with baseless threats of compromise.

The attacker's threat claims that they have linked the anonymized data in the clinical trial to the patient data base. Unless the ransom is paid, the attackers claim that they will contact the patients in the trial who are in the control group to tell them that they have been receiving a placebo and that this situation is preventing them from receiving a successful treatment that would dramatically improve their health prospects.

While XYZ's treatment is showing greater than 90% effectiveness, the results are not sufficient for the FDA to end the trial early and approve the treatment for immediate introduction into the market. Management is concerned that, if the attackers carry through with their threat, the clinical trial will be compromised by both patients and physicians knowing what trial group they are in. Initial estimates indicate that restarting and rescuing the trial in this scenario will cost the company $100M in lost sales and additional trial costs and delay market release by 2 years. In addition to these business concerns are the reporting, regulatory and public relations issues associated with a major HIPAA violation.

CEO Recommendations

- This is obviously a serious event with significant implications for the future of our company. I look forward to your advice and counsel. However, before we open the floor to questions and suggestions, let me tell you what we have done and are planning to do. During this entire situation, our General Counsel and his staff, have been invaluable partners and advisors.
- Immediately after getting the threat, we retained Mandiant's CERT services to confirm the intrusion and determine the extent of the damages which is in process. Mandiant is a subsidiary of Google and one of the country's best known and respected cyber security consulting firms
- My recommendation is that we **not** pay the ransom. It will only leave us open to further extortion and doesn't relieve us of any reporting requirements and the associated publicity. Further, our patients are open to their data being used for identity theft and we have a moral obligation to tell them of the risk and do what we can to mitigate it.
- To support my recommendation, while recent data [1] indicate that the majority of companies (78%) paid the ransom, many were attacked again and 32% paid ransom four or more times during the past 12 months. Further, our threat is primarily reputational and may impact the integrity of our trial; however, unlike many such attacks we are still able to operate. Further, this threat is a very complicated scenario requiring the attackers correlate data from multiple data bases to create havoc to our trial (although compromise of our trial participant personal data is certainly serious in its own right). This complexity increases, in my opinion, the likelihood that it is a creative shakedown rather than a real threat.
- We have retained a PR firm to help us develop a comprehensive communications plan to include our patients and all other public announcements that are likely to be required under HIPAA and SEC rules.
- Relative to our patients this communications will tell them about the penetration and the related risk to their personal data and offer them identity theft protection services to be paid by us. Equally importantly, this communication will tell them that they may be contacted by the hackers telling them their status in the trial; namely, whether they are in the control group or are receiving our treatment. We will ask them to ignore this since the information may not be correct and we can't confirm their status without compromising the integrity of the trial. We are close to completion and are hopeful of a successful result that will clear the way for many patients to get the potential benefits of our new drug. [Still, we will need to balance the possibility that if/when FDA is informed they may view communications, even by third parties, with patient groups about whether they are in the control group will damage the legitimacy of the study results.]

[1] Semperis 2024 Ransomware Risk Report

- We are comparing the current trial database to our latest backup to see if the trial DB has been corrupted by the hackers. If so, we will restore to the last known good configuration and reapply any missed transactions. Fortunately, we store our backup files offsite and offline so we are pretty confident that they haven't been compromised. One of the tasks we will ask Mandiant to complete is to confirm this assumption.
- After we know the integrity of our DB and have our communication plan to patients, we will contact the FDA trial supervisors (this should be take just about a week) to tell them about the situation and our response. We will argue that we think the trial is still valid and should be allowed to proceed to completion.
- We will seek advice from outside counsel and independent accountants about our reporting responsibilities under HIPAA, SEC and any other relevant laws and regulations.
- Now, let's open the floor for discussion.

Questions for the Board

- What should our response be to this threat?
- When do we need to report this threat to the FDA?
- Do we want to/need to issue a press release/make a public disclosure, or SEC filing?
- Do we need to communicate with the patients in our trial? (In this regard, what are our obligations to our patients: statutory, contractual and/or ethical?)
- How should we prepare for the potential negative publicity?
- Pending disclosure to the public (if we decide that), what internal directions should we be providing to employees?
- Is there a way to do this communications that maintains the integrity of the ongoing trial?
- What are our reporting requirements under HIPAA?
- Do we have obligations under State law?
- How does our insurance coverage (cyber, business interruption, general liability & D&O, *if available*) influence our analysis and response to these questions? Should it?

Discussion Questions

- What should XYZ Biotech have done to prepare better for cyber-attack?
- How would the scenario play out differently if XYZ Biotech had subscripted to a hosted service to support its clinical trials?