Ransomware – The Facts

All businesses and organisations are at risk from ransomware. For many of those companies, the risks are substantial and potentially existential, but they are largely contained within the business and its customers. For companies in other sectors, the risks that ransomware poses are much more significant. This includes pharmaceutical companies, making it even more essential for those in the pharma industry to know the facts.

Theoretically, a pharmaceutical company hit by a ransomware attack could see production, quality control, R&D, and other aspects of its operations closed down for a period of time. This will have a direct impact on the business, but it will also have a potentially large impact on the patients who rely on the drugs the company produces up to and including creating life threatening situations.

There could then also be medium and long-term impacts, including ongoing legal and regulatory impacts, as well as the impact of compromised intellectual property.

So, what is ransomware and what do these types of attack look like in their modern form? What are the main risk factors for pharmaceutical companies and what are the essential steps you should take to mitigate those risks and protect your systems?

What is Ransomware?

Ransomware is a specific type of malware designed to lock users out of their devices and systems while also preventing you from accessing data. Cybercriminals often achieve this by encrypting files. The group will then typically demand a ransom to restore your access. The ransom can also come with the threat of releasing your organisation's sensitive data, such as patient or customer data, onto the internet.

Are Pharmaceutical Companies at Risk from Ransomware Attacks?

The answer to this question is a resounding yes. In fact, pharmaceutical companies are a prime target for ransomware attacks.

After all, ransomware attacks are not just about locking companies out of their IT systems. The fact is, cybercriminals who use ransomware attacks like to target companies with highly valuable intellectual property as well as other valuable data, such as patient data. The thinking of the cybercriminal is: the greater the risk they can create for the company, the greater the likelihood of getting paid and the higher the pay-out amount.

This isn't just theory either, as there are many examples of pharmaceutical companies in Europe and elsewhere around the world who have fallen victim to ransomware attacks. We even know some of the names of the groups behind previous ransomware attacks of pharmaceutical companies, including BlackCat/ALPHV, Blackfly, Stone Panda, APT41, and Energetic Bear.

The Financial Cost of Ransomware Attacks on Pharmaceutical Companies

When considering the level of risk for the pharmaceutical industry, it is important to remember that ransomware attacks are not limited to cybercriminals whose aim is to make money. There are also state-sponsored groups that carry out ransomware attacks. For those groups, the motivation is more likely to be geopolitical.

Whatever the motivation of the attackers, there is always a cost. There is potentially no ceiling to the cost of a ransomware attack, but we do have real world examples. One such example comes from a large pharmaceutical corporation that was attacked in 2017. In one quarter of that year alone, the company lost USD $300 million as a result of the attack. The overall cost of the attack, however, is believed to be over USD $1 billion.

How Do Ransomware Attacks Occur?

There are many traditional methods that attackers can use to target a pharmaceutical company with a ransomware attack. The simplest but still, unfortunately, highly effective example is sending emails that contain links to malicious websites. Once the link is clicked, the ransomware program is instantly and secretly downloaded. The attack can then start immediately, or the software could lie dormant for a period of time before it becomes active.

Another common method that cybercriminals use to carry out ransomware attacks is through social engineering. This can take many forms, but it typically involves attackers posing as legitimate individuals and convincing employees to take an action that gets them into the company's systems. The actions of the employee can be malicious but, more often than not, they don’t know they are doing anything wrong.

Additional Risk Factors for the Pharmaceutical Industry

The above two examples of how a ransomware attack can occur applies to all organisations, but there are additional considerations in pharmaceutical companies. This is because pharmaceutical companies don't just have IT – information technology. They also have OT – operational technology. OT is the equipment and systems that run your production lines, laboratories, and other manufacturing-related functions.

It is common in pharmaceutical companies to have a broad range of legacy equipment and systems within their OT infrastructure. These legacy systems and equipment typically don't have the same security features that are standard in modern equipment and systems. This in itself creates cybersecurity risks, but then there is also the push in pharmaceutical companies to modernise operations by integrating systems, automating processes, and making better use of data.

This modernisation of pharmaceutical manufacturing operations brings considerable productivity and efficiency benefits, but it also has the negative impact of increasing the organisation's attack surface, i.e., increasing the potential entry points that an attacker can use to gain access to systems and install ransomware software.

How to Mitigate the Risk of a Ransomware Attack

The main step to mitigate the risk of a ransomware attack is to work with third-party IT companies and cybersecurity professionals to ensure your systems and processes are as robust as they can be.

Other crucial tips that can help protect your pharmaceutical facility from a ransomware attack include:

- Make sure staff receive regular, high-quality training on cybersecurity, especially in relation to the social engineering techniques that attackers use. This should include phishing simulation tests where staff are presented with potential attack scenarios to see how they respond. This is a valuable learning experience, and it will give you an ongoing understanding of your preparedness.
- Implement complex passwords for all users and all systems and equipment.
- Implement multi-factor authentication.
- Design and implement access control policies to ensure staff, contractors, and other third parties only have access to the systems and data they need.
- Implement network segmentation to enhance monitoring and oversight and make it easier to isolate compromised devices and equipment.
- Monitor user behaviour to identify deviations from the norm. For example, a lab technician or a member of staff in accounts is unlikely to be using a tool like PowerShell, Microsoft's task automation and management program. If monitoring activities identify they are using a tool like this, it should be investigated.

- Backups are essential, but the sophistication of modern ransomware attacks often results in online backups also being compromised. Therefore, offline and encrypted backups should also be maintained.
- Stress test ransomware attack recovery processes to identify weaknesses and make improvements.

Finally, it's important to re-emphasize the importance of the point above in relation to staff training. After all, cybersecurity in your organisation is only as strong as your weakest link, and your weakest link is likely to be your people.

Maintaining a strong security posture and staying proactive in the face of evolving threats, both technically and on a human level, is crucial to safeguarding your organisation against ransomware attacks.