Increase vigilance against cyberattacks

The biotech sector must devote more resources to cybersecurity — especially those companies that are manufacturers of essential medical products.

Cyberattacks are on the rise. Since the WannaCry and NotPetya computer worms wrought mayhem across the globe, digital attacks are becoming increasingly commonplace. Today, the US government says healthcare cyberthreats account for 24.5% of all hacks — more than for any other sector — with each breach costing an average of ~$5 million. And in healthcare, the biotech sector may be the weakest link of all. With its data-intensive R&D programs, high-value intellectual property, complex cold-chains, distributed manufacturing systems, and market monopolies on the one hand, and numerous externally facing collaborations and weak cybersecurity resourcing on the other, it appears ripe for cybercrime. Most worryingly for companies manufacturing life-saving products like insulin or replacement proteins, a failure to secure computer networks could turn out to be a matter of life and death for patients.

Digital attacks can take many forms: deliberate sabotage of computer systems; cyberespionage to gain unauthorized access to proprietary information; and ransomware to lock a computer network or encrypt files with the aim of extortion. Perpetrators may be nation state actors with geopolitical motivations (including the United States); hacker groups or criminal gangs that pool resources and expertise with the aim of extorting victims; or lone wolves motivated by mischief, a personal grudge or some other agenda.

Several lines of attack are employed: phishing (en masse or targeted, 'spear phishing' e-mails that lure users to click a link or open an attachment depositing malware onto the target system), smishing (deceptive SMS texts with a similar aim), hijacking of remote desktop protocols (used by administrators on company networks), exploiting cloud and software vulnerabilities (which are constantly being discovered and patched), 'watering hole attacks' (malicious websites that deposit malware onto the computers of unsuspecting visitors), and external devices like memory sticks that can be used to physically upload malware into a network.

According to cybersecurity experts Bitdefender, ransomware attacks spiked by an astounding 485% at the beginning of the COVID-19 pandemic, many of them affecting biopharma companies. Lockdowns, remote working and increased use of unsecured VPNs (virtual private networks), together with a wealth of proprietary R&D behind biotech vaccines, antibodies and diagnostics, have placed biotech companies in the crosshairs.

In October 2020, Dr Reddy's Laboratories was forced to shut several production facilities in the wake of a data hack, just as it geared up for late-stage trials on Russia's Sputnik V vaccine. Around the same time, hackers impersonating an executive from China-based Haier Biomedical sent spear-phishing emails to several different companies involved supporting the vaccine cold chain. North Korean hackers posing as job recruiters on LinkedIn and WhatsApp approached AstraZeneca employees working on the COVID-19 vaccine with fake job offers in the hope of accessing victims' computers; and according to *The Wall Street Journal*, these same hackers were also responsible for attempting to steal vaccine information from Johnson & Johnson and Novavax, as well as three South Korean drugmakers. In December 2020, Pfizer announced it had been informed the European Medicines Agency that documents relating to its Comirnity COVID-19 vaccine had been unlawfully accessed; they were later released. And in 2021, a malware attack — 'almost certainly' attributed to Russian intelligence services — caused a two-week network outage at Miltenyi Biotec, which was sequencing COVID-19 samples for research.

These are the attacks we know about. Many more likely do not get reported because of the reputational damage involved. But one cyberattack above all others serves as a learning moment.

In 2017, NotPetya infected Merck's central computer network, taking down ~30,000 computers and encrypting data across sales, manufacturing and research. The attack paralyzed the drugmaker for two weeks and affected computers controlling production of its human papilloma virus and hepatitis B vaccines, resulting in supply shortages. Merck ended up having to borrow $240 million worth of Gardasil vaccine from the US Centers for Disease Control's stockpile, with overall losses calculated at >$1.0 billion. It took till January of this year for the pharma to be paid out by its insurers.

Given Merck's experience, cyberthreats to the manufacture of several other biotech drugs should be of especial concern.

Taking insulin as one example, at least 42 independent companies manufacture insulin worldwide. But in the United States, a persistent oligopoly of just three companies—Novo Nordisk, Sanofi and Eli Lilly—is responsible for all the supply. If cybercriminals took out manufacturing facilities at these three companies, the US insulin supply could be severely compromised.

Similarly, drugmakers manufacturing recombinant enzyme replacement therapies may also be targets. Tens of thousands of patients with rare diseases depend on enzyme therapy. And yet a survey of approved enzyme replacement therapies shows that just eight manufacturers provide the majority of these products. We already know the dire consequences of shutdown at one of these manufacturer's plants: a decade ago, adventitious viral contamination at Genzyme (now Sanofi) led to crippling drug shortages for people with Gaucher's and Fabry diseases. Why would a cyberattack not lead to similar consequences?

Luckily, there are signs that the US government and industry groups are awakening to the threat. Last year, the Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) was founded to provide members in both the private and public sector with threat intelligence, vulnerability identification and mitigation, and education and outreach. Similarly, the Biohacking Village provides a place to interact with 'white hats' — hackers who seek to work with companies to probe cyber vulnerabilities in networks and provide patches to secure systems.

But the entire biotech industry needs to raise its awareness. Just this June, the 'Industrial Spy' data-extortion gang put up for sale on the group's Tor extortion marketplace files stolen from Novartis, which it priced at $500,000 in bitcoins. For cyberattacks and data breaches, biopharmaceutical companies must accept that it is a matter of when, not if. ❐

Published online: 3 August 2022
https://doi.org/10.1038/s41587-022-01446-4