Biotech and pharmaceutical firms hold vast amounts of valuable data and information making them prime targets for cyber-attacks - so how are they protecting themselves?

In the American political thriller series, Homeland, a vice presidential candidate's pacemaker was attacked by offshore terrorists, inducing a heart attack that resulted in his untimely death. In the real world, when Dick Cheney was serving as the 46th vice president of the United States between 2001 and 2009, he famously deactivated the connectivity on his pacemaker so as to prevent anything similar from taking place.

The threat to medical devices may seem like the stuff of science fiction, but in the US, healthcare is now the largest target of cyber security attacks, reportedly at greater risk than manufacturing and banking[1]. According to experts, the value of stolen personal health information is ten to twenty times greater than the value of a stolen credit card number.

**Valuable data**

*Life science* companies hold vast amounts of critically important data and information. Obvious categories include data arising from the development and testing of pharmaceutical products, including clinical trial data, while the rise of biologic drugs has also brought with it valuable manufacturing know-how for these complex molecules.

The sophisticated nature of medical devices and their connectivity raises additional risks. Add in commercially sensitive information about products and their pricing and promotion, and it's no
surprise that the sector finds itself the target of cyber-attacks.

Josh Hanet is a senior associate at Gowling WLG, based in Toronto, with a practice focused on medical defence law. He says healthcare cyber security is becoming a significant area of concern for medical device manufacturers and regulators tasked with protecting the public.

"So far, most of the examples in Canada and the US have been ransomware attacks, where hospital networks are attacked and a bitcoin ransom is demanded. There is a potential loss of data, and a risk that hackers have gained access to potentially significant personal health information."

Cyber-attacks as a global issue

In Europe and elsewhere, cyber-attacks are increasing thanks to the growing volume of electronic data and the rising use of electronic storage to keep data. Adding to the problem is the sophistication of cyber criminals.

Helen Davenport is a director based in Gowling WLG’s London and Birmingham offices, specialising in technology-related commercial disputes, including cyber-crime and data breaches. She says: "In life sciences, there is an employee threat, where insiders may want to make use of information that they have access to, whether it is intellectual property or personal data.

"Another potential motivation is around sabotage and public profile, where there are people with grudges against pharma companies who want to cause those companies harm by disrupting their businesses and generating bad press."

Key cyber security threats

Patrick Duxbury, partner and head of life sciences with Gowling WLG in the UK, says pharma and biotech companies are concerned about cyber security threats in three key areas:

- Data relating to clinical trials, and particularly patient data generated during clinical trials. This data is incredibly sensitive at both the patient level and at a commercial level.
- Corporate know-how and confidential information relating to the manufacture of biologic drugs.
- Day-to-day commercially sensitive information regarding drug pricing and promotion - a hot topic given the pressures on healthcare budgets around the world.

Duxbury says: "The explosion of large molecule drugs in the last 20 years has created new
categories of very valuable information. These drugs are very difficult to make which means companies are very keen to protect their intellectual property and trade secrets. If that information is hacked, or becomes public, that would be incredibly damaging from a commercial point of view. The increasing value of trade secrets has been recognised in both the US and Europe with major legislative changes coming into force this year to enhance the statutory protection available to prevent misuse."

He adds: "Companies see themselves at risk of people hacking into their systems and stealing their know-how, and there has been a huge spike in cyber-attack attempts being made on pharmaceutical systems."

**Regulators and cyber security**

Regulators have a significant role to play in protecting the public from the impact of cyber security breaches. Both the American Food and Drug Administration (FDA) and European lawmakers have made regular calls for companies to tighten their systems.

The FDA has taken the lead recently in enacting legislation to address manufacturers who fail to properly prevent or rectify a cyber security risk to medical devices. Failure to comply can now see devices disapproved, recalled, or face regulatory or legal action.

In January 2016, the FDA published draft guidance for the post-market management of cyber security in medical devices, emphasising the need to keep on top of the threat from hackers even after devices have been deployed. The post-market considerations that are critical to the FDA include:

- Monitoring cyber security information sources for identification and detection of cyber security vulnerabilities and risks;
- Understanding, assessing and detecting presence and impact of vulnerabilities;
- Establishing and communicating processes for vulnerability intake and handling;
- Defining essential clinical performance to develop programs that protect, respond and recover from the cyber security risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cyber security risk early and prior to exploitation.

It has also called for more collaboration between all the various stakeholders in the industry - including the IT community, manufacturers, and clinical users - to combat cyber-crime.

Hanet says: "Many of the regulators around the world are quite reactive, but the FDA is proactive, so we advise clients to look to what the FDA is doing, because where it leads, others
often follow. We are seeing obligations now not just when developing devices, but also once they have hit the market. Just like the iPhone gets constantly updated as new threats emerge, now medical devices that have been deployed need to be considered in a similar way."

**Information risk management**

In the UK, life sciences businesses should be aware of the guidance available that deals with information risk management. For example, the government's information risk management regime puts forward 10 Steps to Cyber Security[2].

The government advises boards to establish an effective governance structure, maintain board engagement with cyber risk, and produce supporting information risk management policies.

"A lot of the guidance is around personnel, training, understanding the threat and having a comprehensive strategy in place to deal with it," says Davenport. "The threat is becoming ever-more sophisticated particularly when it comes to assets such as high-value know-how and clinical data, but equally the statistics show that many incidents involve either insider threats, or employee failure.

"My advice is to start at a fairly basic level with things like user education, network security and mobile working policies, and then develop a strategy to cover more sophisticated threats if necessary, to ensure the crown jewels of your business are protected."

**Fragmented legislative framework**

The contributions of the FDA and the UK government form just a small part of a legislative framework that is very fragmented, both in terms of laws and standards. An example is ISO 27001[3], an information security management standard published in October 2005 by the International Organisation for Standardisation.

This standard aims to bring information security under explicit management control so that organisations that have signed up can be formally audited to ensure they are compliant with the standards set. Meanwhile, the Medicines and Healthcare Products Regulatory Agency (MHRA) in the UK has also issued draft guidance over medical devices this year to take into account recent developments in apps.

At the European level, the Network and Information Security Directive[4], otherwise known as the Cyber Security Directive, entered into force in August 2016, and member states now have 21 months to adopt its rules into national legislation.
Duxbury says: "Cyber security is very much a cross-border issue and this industry is about as international as you can get. There have been attempts across the globe to try to achieve standardisation of approach internationally, but for now companies are faced with a patchwork of legislation, regulations and guidance."

**Monitoring the cyber threat**

Industry will need to commit more resources to managing cyber risk as the threat continues to evolve. Three large US health insurance firms - Anthem, Premera Blue Cross and UCLA Health - have recently suffered headline-grabbing cyber-attacks concerning patient data.

Indeed, IBM research\(^5\) says 100 million medical records were compromised globally in 2015 alone. During the most recent Olympics, the World Anti-Doping Agency said Russian hackers broke into its network and released personal medical records of several top international athletes.

When it comes to the critical area of intellectual property, a PwC survey\(^6\) recently found theft of intellectual property (IP) in cyber-attacks on life sciences and pharma companies skyrocketed 176% in 2015, with many stories of hackers selling IP from life sciences firms.

"You mention cyber security and everybody's ears perk up," says Hanet. "It is on their radar, but can become a black hole as you can't possibly be on top of every threat. As technology evolves, so do the threats, often at a pace that is faster than companies can keep track of. From a regulatory perspective, companies are trying to keep ahead of the curve, and from a legal point of view, there's a concern that you are only ever one attack away from significant liability."

For now, best practice centres on the continuous monitoring of the threat, assessing and detecting vulnerability, establishing processes to address weaknesses, adopting disclosure policies, and developing and deploying mitigations when necessary.

For medical devices, the post-market management of risks is becoming as important as the pre-market - particularly if vice presidential health scares are to remain only in the realm of TV dramas.

**Footnotes**

2. [https://www.ncsc.gov.uk/guidance/10-steps-cyber-security](https://www.ncsc.gov.uk/guidance/10-steps-cyber-security)
This article first appeared in April 2017 edition of European Pharmaceutical Review.

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.

Related Life Sciences

Author(s)

Helen Davenport  
Partner - Birmingham  
Email helen.davenport@gowlingwlg.com  
Phone +44 (0)121 393 0174  
vCard Helen Davenport

John Norman, PhD  
Partner - Leader of Life Sciences Group, Ottawa  
Email john.norman@gowlingwlg.com  
Phone +1 613-783-8848  
vCard John Norman, PhD

Josh Hanet  
Partner - Toronto  
Email josh.hanet@gowlingwlg.com  
Phone

Patrick Duxbury  
Partner - Head of Life Sciences (UK), Birmingham  
Email patrick.duxbury@gowlingwlg.com
Gowling WLG is an international law firm comprising the members of Gowling WLG International Limited, an English Company Limited by Guarantee, and their respective affiliates. Each member and affiliate is an autonomous and independent entity. Gowling WLG International Limited promotes, facilitates and co-ordinates the activities of its members but does not itself provide services to clients. Our structure is explained in more detail on our Legal Information page.

© 2020 Gowling WLG International Limited. All rights reserved.