Digital Health and Cyber Risk in the "New Normal"

The Risk Landscape for Life Sciences:

Life sciences organizations are one of the more at-risk sectors for cyberattacks, which have increased significantly from pressures imposed by the COVID-19 pandemic.

- Recent research has found the life sciences sector risk from direct cyberattacks may reach US$642 billion by 2024 — second only to the high-tech sector. Pandemic-related remote working has increased security vulnerabilities, and organizations have had to quickly onboard or reconfigure arrangements with third parties which have opened up new risks in the supply chain.

- Urgent government warnings to life sciences organizations state that nation-state attackers are directly targeting COVID-19 research and valuable intellectual property (IP). Cyberattacks have increased exponentially since the COVID-19 pandemic began, targeting remote workers with phishing attacks. Recent ransomware attacks have shut down production lines at life sciences firms and ramped up extortion attempts by stealing and threatening to expose highly sensitive personal data.

The excitement of the digital revolution in technology innovation and digital health also comes with complex legal and compliance risks that must be carefully navigated.

- In addition to privacy rules such as GDPR, life sciences organizations must contend with an increasingly complex web of regulations that affect their core businesses, including brand rules around new technologies such as artificial intelligence (AI), medical device Internet of Things (IoT), and digital health applications. Moreover, there is increased risk that group litigation claims — including for nonfinancial losses such as emotional distress — that may follow a cyberbreach or exposure of sensitive personal data such as patient records.

- There is also increased focus on who has access to life sciences data and who owns or controls that data. This is a key issue following the *Schrems II* decision by Europe's highest court on July 16 that invalidated the EU-U.S. Privacy Shield and questioned other transfers of personal data from the EU/UK to the United States and other countries.

Practical Steps to Manage Risk:

1) Take additional steps to ramp up cybersecurity at your organization. Now is the time to work at pace to identify and resolve security vulnerabilities, examine whether endpoint detection and monitoring tools are sufficient, and consider red team testing — using ethical hackers to simulate attacks and test your defenses. Your employees are being targeted, so consider ramping up security awareness training as well.

2) Take steps to secure your vulnerabilities through third-party partners and suppliers. Now is the time to assess your third-party relationships for cyberrisks, including updated security questionnaires, technical audits, contractual security obligations, and threat intelligence monitoring of critical suppliers.

3) Have a strategy to protect all categories of data: personal data, confidential business data, IP, and trade secrets. You will need to work out what the complex web of regulations requires, identify what information you hold that is most valuable, create a record of it, and then take specific measures to protect each category. You should have a detailed incident response plan that is well-tested and reviewed regularly, plus qualified third parties in legal and incident response to help vet it.

4) Ensure you have a solid digital governance strategy. Emerging regulations on technology innovation and privacy mandate a risk-based approach, which will require formal audits and due diligence, mitigations, and accountability from senior management. Consider appointing a chief digital officer or digital governance committee and align strategy with related functions such as cybersecurity and business continuity.

5) Take immediate steps to address the impact of the European Court of Justice's decision on July 16 in *Schrems II*. Organizations should immediately take steps to address the impact of this important decision, which invalided the EU-U.S. Privacy Shield and requires an assessment of the level of privacy protection in the countries outside of the EU where data is transferred to. Organizations should be looking very carefully at where data is transferred and who has access to it, consider alternative transfer mechanisms, and review their standard contractual clauses with partners and suppliers.

6) Test cyberattack scenarios ahead of time and often. Organizations should be regularly testing their incident response plan through tabletop exercises with management. A financial impact assessment of common scenarios is also recommended — such as a patient data loss, ransomware attack, or downtime for a production facility — to ensure you have a plan to finance a response, business interruption, customer churn, or follow-on litigation.

7) Finally, be prepared to do things differently. We are in a rapidly changing world, and adaptation is critical. You can expect to do more audits, perform enhanced due diligence, and appoint leaders to new responsibilities. Be prepared to defend your organization's strategy and response in multiple contexts, and from the highest levels of your business.

Contacts:

William Long
Partner, Co-leader Privacy and Cybersecurity Practice
Sidley Austin LLP
wlong@sidley.com
+44 20 7360 2061

Vishnu Shankar
Senior Associate
Sidley Austin LLP
vshankar@sidley.com
+44 20 7360 2067

Spencer Lynch
Managing Director
Aon's Cyber Solutions
spencer.lynch@aon.co.uk
+44 75 3846 8636

Chris Scott
UK Deputy Practice Leader
Aon's Cyber Solutions
christopher.p.scott@aon.co.uk
+44 20 7086 0795

Brandy Wityak
Vice President
Aon's Cyber Solutions
Brandy.Wityak@aon.co.uk
+44 75 0851 5216