Cyber Resiliency

PhRMA member companies remain dedicated to researching, developing, and delivering lifesaving and quality-of-life enhancing innovations for patients, which includes maintaining a robust cybersecurity infrastructure throughout their global supply chains to ensure access to medicines. There are a range of ways PhRMA member companies work to bolster cyber resiliency, including using advanced analytics for product tracking and transparency, conducting cyber risk assessments across their supply chains, including vendors and suppliers.

Understanding Cyber Resiliency

Pharmaceutical companies face a range of threats related to cybersecurity, including coordinated cyber threats from nation-state hackers, criminal ransomware efforts, or (witting or unwitting) lapses in internal processes. Cyber threats have been on the rise for several years, and since the onset of the pandemic, there have been an even greater number of concerted efforts by foreign actors to access critical research or disrupt the United States' healthcare infrastructure. To encourage resiliency across cyber operations as firms become increasingly digital in nature, PhRMA member companies are continuing to implement a range of activities, including ongoing supplier risk assessments, applying advanced analytics for product tracking and transparency, and using holistic approaches to defend against ongoing cyber threats.

The Importance and Objectives of Cyber Resiliency:

A high-level scan of PhRMA member company websites and publications finds that all 32 member companies are continuing to actively invest in cyber resiliency at some level. Examples of activities include elevating cybersecurity leadership to C-suite levels; robust cyber strategies and security operations with emphasis on preventive and proactive measures (e.g., cyber-assessments, cyber-war gaming and cyber-incident response); "zero trust" security frameworks that require all users to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data; third-party risk assessments in supply chain and distribution to enhance cybersecurity internally and across vendors and suppliers; and continual security awareness sessions and assessments of effectiveness. As a result of these activities, investments in cyber resiliency for biopharmaceutical companies are designed to:

Protect Data: Biopharmaceutical companies make significant investments to manage legal regimes of data protection, privacy, and cybersecurity across markets.

Improve consumer trust and transparency: Because trust is essential to all business relationships, opportunities to enhance the trust between companies and consumers is key. As improved cyber resiliency offers companies an enhanced understanding of their value chain, an added benefit is transparency. Biopharmaceutical companies are active stewards of cybersecurity, and as a result, there is an added benefit of cyber resiliency that helps build consumer trust.

Avoid business disruptions and resulting economic burdens: Beyond potential reputational harm, cyber threats can also yield financial costs. In addition to improving trust, safety, and transparency, activities that encourage cyber resiliency can help companies mitigate resulting economic burdens related to cyber-attacks.

Cyber Resiliency: Examples of PhRMA Members in Action

To overcome these threats, the biopharmaceutical industry is taking critical measures to enhance its cybersecurity posture. Research finds that all PhRMA member companies are deploying measures to ensure cyber resiliency, ranging from developing cybersecurity strategies, working on zero trust platforms that combine network, data, and access information, investing in third-party risk assessments for both technology and processes to enhance their ecosystems, or hiring specialized cybersecurity professionals.[1]

Underlying these high-level counts, notable examples of PhRMA member companies working to ensure cyber resilience are highlighted below:

HEALTH INFORMATION SHARING AND ANALYSIS CENTER

In 2021 and 2022, six PhRMA members companies (Amgen, Johnson & Johnson, Eli Lilly and Company, Merck, Pfizer, and Takeda) participated on the board of directors of the Health Information Sharing and Analysis Center (Health-ISAC), a community of critical infrastructure owners and operators within the healthcare and public health sector focused on sharing timely, actionable, and relevant information.[2] According to the most recent Health-ISAC Annual Report, 85% of the top 25 pharmaceutical manufacturers are participating members. The Health-ISAC community is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material. Health-ISAC working groups and committees focus on topics and activities of importance to the sector and produce white papers for public sharing. Health-ISAC is constantly engaged with external partners such as government, law enforcement, the vendor community, and other associations (e.g., HIMSS, MDISS, EHNAC and CHIME) to facilitate situational awareness and inform risk-based decision making to protect the HPH and other critical infrastructure sectors.

ENSURING CYBERSECURITY COMMITMENTS

Novartis is ensuring commitments from its suppliers to implement robust cybersecurity layers across the supply chain.[3] Novartis includes cybersecurity in its Code of Ethics commitments, the company's guiding principles intended to ensure honesty and integrity in all facets of operations. Novartis also requires their suppliers to implement organizational security policies and standards. To prevent system interruptions, Novartis has extensive business continuity plans that are tested at regular intervals, while also conducting internal vulnerability analyses and third-party testing to ensure the effectiveness of controls.

ANALYZE SAFETY RISKS

Bayer regularly analyzes safety risks and implements robust identification, prevention and processing measures, including employee training and information measures pertaining to cybersecurity as part of its Enterprise Risk Management.[4] Safety and crisis simulation exercises are also regularly conducted, and each year, Bayer works with IT service providers to test the restoration of IT systems and global data centers.

COUNTERING CYBER RISKS

To counter the risk of cyberattacks, Otsuka employs several measures, such as arranging system security audits by external specialists, diagnosing website vulnerabilities, conducting drills related to targeted email attacks, and monitoring posts on social media.[5] The group also conducts regular emergency drills with a focus on the core systems that construct data. In addition, Otsuka has built capabilities for responding to cybersecurity emergency situations, including the establishment of the Computer Security Incident Response Team (CSIRT), which preempts the occurrence of damage from cyberattacks targeting personal information and trade secrets held by respective group companies.

USING A MULTIFACETED STRATEGY

UCB has a multifaceted cybersecurity and data management strategy, along with active programs for the proper prevention, detection and response controls.[6] This includes continuous monitoring and analytics, intrusion incident detection and response, security testing and user awareness training and campaigns. Additionally, UCB has a Cyber Crisis program that allows the company to properly handle large security incidents (e.g., data breach or malware). UCB has established robust processes, procedures, and controls to continue to comply with global best practices for privacy and data protection. In addition, UCB liaises with regulators and industry associations to remain abreast of developments as this dynamic area continues to evolve.

AWARENESS AND COMPLIANCE TRAINING

Amgen employees receive annual security awareness and compliance training that includes information on applicable data security and privacy laws and regulations and the appropriate handling of personal information.[7] The global training programs are available in 24 languages. Amgen also hosts regular employee awareness events and campaigns on topics such as ransomware, identity theft, and mobile security, and conducting internal phishing exercises. To keep employees educated and engaged on cybersecurity, Amgen launched a series of virtual cyber escape rooms in 2021, where teams compete to solve security challenges.

CONTINGENCY PLANNING

Novo Nordisk is continuing to introduce a range of actions to encourage cybersecurity, including company-wide information security awareness activities, contingency plans for non-availability of IT systems, company-wide internal audit of IT security controls, and detection and protection mechanisms in IT systems and business processes.[8]

1 TEConomy Partners analysis of PhRMA Member Companies
2 Health-ISAC Inc., "Health Information Sharing and Analysis Center." See: https://h-isac.org/
3 Novartis, "Novartis in Society: Integrated Report 2021." See: https://www.novartis.com/sites/novartis_com/files/novartis-integrated-report-2021.pdf
4 Bayer, "2019 Sustainability Report." See: https://www.bayer.com/sites/default/files/2020-12/bayer-ag-sustainability-report-2019_5.pdf
5 Otsuka, "Risk Management." See: https://www.otsuka.com/en/csr/governance/risk_management.html
6 UCB, "Integrated Annual Report 2021." See: https://www.ucb.com/sites/default/files/2022-02/2021_UCB-Integrated-Annual-Report_ENG.pdf
7 Amgen, "Cybersecurity and Data Privacy." See: https://www.amgen.com/responsibility/a-healthy-amgen/cybersecurity-and-data-privacy
8 Novo Nordisk, "Annual Report 2022." See: https://www.novonordisk.com/content/dam/nncorp/global/en/investors/irmaterial/annual_report/2023/novo-nordisk-annual-report-2022.pdf