ISG®

Cybersecurity in Life Sciences in the Time of War and Pandemic:

5 Ways to Mitigate Risk

Sameer Nanda and Alok Tripathi

ISG WHITE PAPER

INTRODUCTION

The Life Sciences industry has undergone a massive transformation in the last two years. Decentralized clinical trials, new digital channels of engagement for healthcare professionals, patients and employees, remote monitoring of assets and automation – these are some of the many items that have moved to the top of the CIO agenda. While there is increased pressure to quickly adapt to a new way of working, the current enterprise architecture and IT environment create vulnerabilities to cyber-attack.

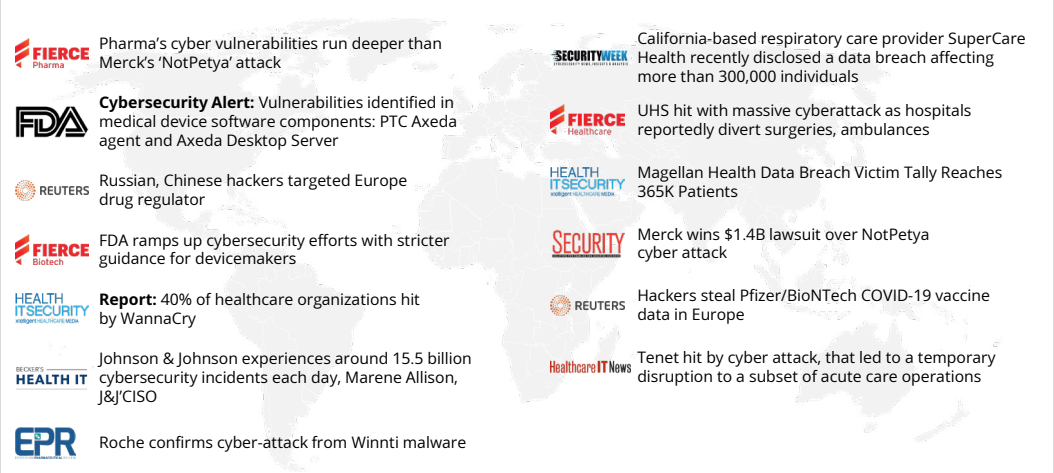
Average total cost of a cyber breach in 2021: $4.24M

Average time to identify and contain: 280 days

Cyber-crimes are not alien to the Life Sciences industry. For 11 consecutive years, Healthcare and Life Sciences have topped the list of data breach costs. According to the IBM-Ponemon Institute 2021 Cost of a Data Breach Report, the average total cost of a data breach in 2021 was $4.24M. That's up from $3.86M in 2020. The average cost of a data breach in the Healthcare industry in 2021 was $9.23M and in the Life Sciences industry in 2021 was $5.04M. Several high-profile attacks in the last decade targeted the Life Sciences industry: the Dragonfly attack in 2014 (which targeted manufacturing industrial control systems); the NotPetya attack in 2017 (which was linked to the Russia-Ukraine conflict and disrupted Merck's vaccine production, resulting in damages in excess of $1B); the WannaCry attack in 2017 (which affected the healthcare systems in 150 countries), the Winnti attack in 2019 (which affected Roche and Bayer) and the security breach of the European Medical Agency in 2020.

Due to the value of health data and intellectual property, the impact to society and the highly profitable global Life Science business, organizations have always been lucrative targets for cyber criminals. Recent developments in the last three years have expanded the attack surface even further and increased the industry's vulnerability to cyber attacks.

Figure 1: Notable News on Cyberattacks and Third-party Security Breaches in the Healthcare and Life Sciences Industries



Source: ISG

Decentralized Clinical Trials (DCT) and Telemedicine

Pre-pandemic adoption of DCT and telemedicine has been tepid due to regulatory and data security requirements. The number and expediency of clinical trials reduced drastically due to limited physical access of patients and physicians. Clinical trial software company Medidata estimates an 80% drop in patient enrollment between March 2021 and March 2020 due to COVID-19. The Life Sciences industry was forced to accelerate DCT by rapidly adopting remote consent, remote monitoring and collection of data. As per one survey conducted by Veeva Systems, during the pandemic, 87% of sponsors and CROs deployed DCTs to manage and advance clinical studies (compared with 28% pre-COVID).

To adapt to travel restrictions caused by the pandemic, Life Sciences organizations moved DCT/telemedicine to the top of the agenda. On the one hand, these have emerged as solutions that provide more independence to patients and caregivers alike. On the other hand, the use of a plethora of connected devices, networks and interfaces to interact and collect data increases the vulnerability for cyber-attacks.

Rise of IoT and IIoT

Lately, pharmaceutical and medical device organizations have heavily invested in IoT and IIoT initiatives. During the pandemic, Life Sciences organizations went through a challenging time, when access to key personnel in manufacturing units was disrupted. Employees who had knowledge of critical equipment in aging units were either absent or physically unavailable to run and/or fix assets. This forced organizations to rapidly deploy remote monitoring, remote operations and automated solutions. But the connected ecosystem of assets and expanded software applications and access points exposed vulnerabilities to attack on individual devices/applications and much larger industrial control systems. These are threats that can cripple an entire manufacturing unit and cost an organization millions of dollars.

Rapid Adoption of Cloud Computing

We have seen unprecedented investment in cloud adoption in the Life Sciences industry in the last three years. This trend will continue as organizations move from on-premises to cloud-hosted solutions to achieve flexibility, transparency and cost control. Traditional hosting on-premises is not necessarily more secure than cloud security. However, overreliance on built-in security tools, suboptimal configuration and compromised implementation quality for speed to market can open up vulnerabilities that can be used as a point of breach for cyber criminals. According to the Ponemon Report, cloud misconfiguration was one of the common attack vectors, contributing to 15% of total attacks in 2021. Furthermore, organizations that have prioritized a robust implementation of their cloud migration are able to identify and contain breaches much faster than peers with lower maturity.

The Impact of Work-from-home on Life Sciences Security

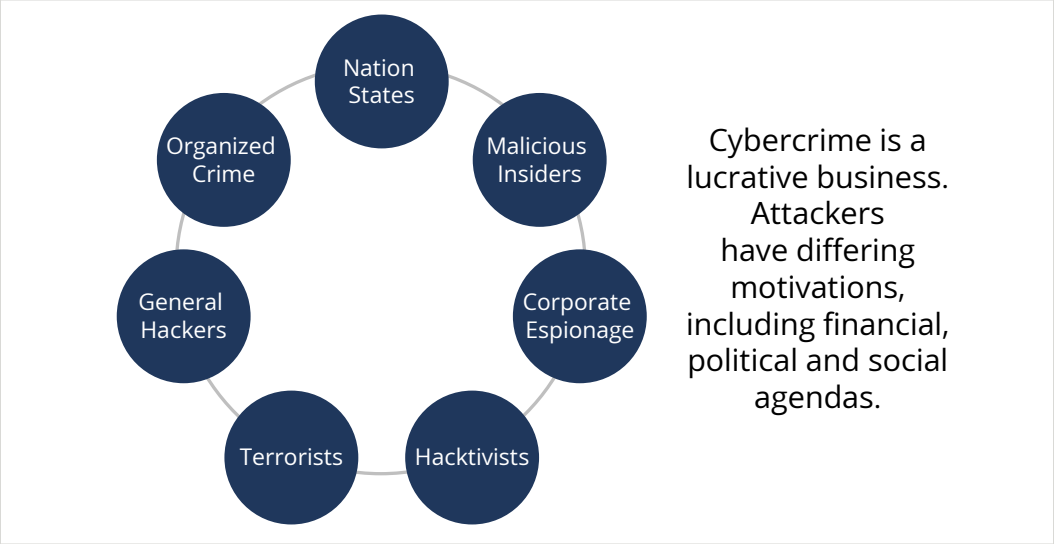
Like other industries, the Life Science industry rapidly adopted remote working after the outbreak of COVID-19. This includes staff from IT operations and development and from internal organizations and service integrators alike. Research conducted by IBM/Ponemon Institute found that the new work-from-home model has adversely affected cybersecurity. In 17.5% of organizations, remote work was linked to a breach, and for breaches in which remote work was a factor, the average cost was $1.07M higher. This unprecedented shift led to a vulnerable hybrid workplace with a broadened attack surface. Organizations that didn't implement digital transformation programs to adequately address COVID-19 challenges ended up paying $750,000 higher per breach than those that implemented transformation programs to address COVID-19 related changes.

The Impact of Geopolitical Instability and Conflict on Life Sciences Security

The past three years have seen multiple overlapping issues threatening geopolitical stability. Among other risks there has been an increased risk of targeted cybercrimes and espionage.

The NotPetya attack in 2017 that crippled Merck's HPV vaccine production was seeded during the Russia-Ukraine conflict earlier that year. The current, overlapping conflicts across the globe (including but not limited to the ongoing Russia-Ukraine conflict) is an ideal breeding ground for new and more sophisticated cyber threats. Whether because of a targeted attack due to the nature of the business of the Life Sciences industry or due to collateral damage, the risks are very high.

Figure 2: Types of cyber attackers



Source: ISG

To learn more about how the geopolitical situation is affecting cybersecurity of Life Sciences organizations, read the latest article by ISG.

What Can Life Sciences Enterprises Do to Reduce Cybersecurity Risk?

Here are the top five cybersecurity priorities for Life Sciences companies:

1. **Boost your data security and data loss prevention (DLP).** Post pandemic, as Life Sciences organizations move their applications to the cloud at an accelerated pace, most IT, OT and IoT systems are running in a multi-cloud environment (hybrid, public, private, etc.). Greater reliance on suboptimal configurations can lead to increased vulnerabilities. To add to that, remote work has given cyber criminals a greater attack surface and opportunity to exploit these vulnerabilities. Organizations should actively consider a risk-adaptive approach to data security and DLP with proactive controls and enhanced use of integrated and cloud-native DLP. Put dedicated effort into identifying and classifying various data sets (clinical/molecule data, health data, key data related to sensitive manufacturing plants) and thoroughly assess risks. Try to identify if the data is at rest, in motion, in use or in cloud and what the access points are. This step is very crucial for research, manufacturing, supply chain and patient data (including any other personally identifiable information). Focus on reducing impact of data loss per classification, device and implement controls.

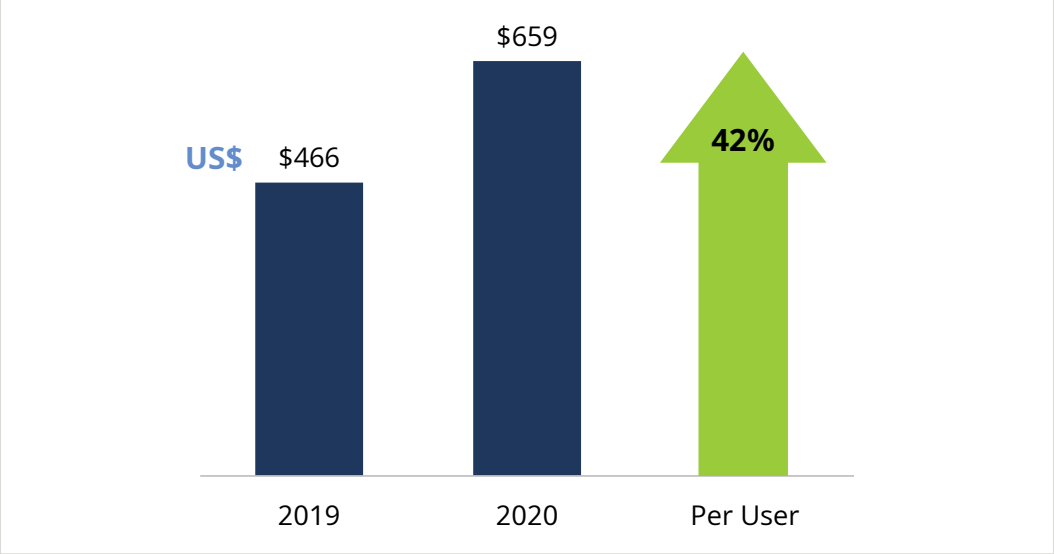
2. **Validate your resilience.** As ransomware attacks evolve and the threat vectors constantly change, organizations need to evolve their resilience plans. In multiple cases, we have seen that attackers are successful in affecting both production and backup systems and organizations have suffered twice from the same attack (e.g., Wannacry). Resilience plans should be designed to ensure uninterrupted protection of "crown jewels," recovery of data, systems in various ransomware attack scenarios and business continuity plans (BCP) for the affected business processes. Not everything can be protected with the same degree of resilience. For example, protecting secret information related to a new molecular entity or a sensitive clinical trial that can determine approval of a potential new blockbuster will need greater protection than "call metrics" populated from a CRM system. Conduct a business impact analysis and prioritize assets and business processes accordingly. Understand the dependencies and requirements and test plans for disaster recovery (DR) and BCP for all scenarios regularly.

3. **Establish a risk-based lines of defense (LoD) model.** While Life Sciences organizations transform to enable work from home, run DCTs or enable digital threads for a digital manufacturing unit, it is essential they consider a risk-based product strategy with cybersecurity embedded in the end product from the beginning of the product lifecycle. For example, the architecture for telemedicine or DCT should include:
   - Clear segregation of duties and controls (including right tooling) at every line of defense.
   - A vulnerability assessment for platform, network and software of individual connected instruments.

4. **Ensure convergence of IT, OT and IIoT.** The Life Sciences industry is rapidly amalgamating industrial operational technology (OT), industrial internet of things (IIoT) and information technology (IT). As a consequence, the cybersecurity threat landscape is becoming more and more complicated and widening the attack surface. There is also a lack of widely accepted standards, integrated digital forensics, methodologies, maturity models or processes. On top of this, IoT botnets are growing in both size and power and are increasingly capable of unleashing powerful attacks, as application distributed denial of service (DDoS) is overtaking network DDoS. Organizations procuring third-party tools for their OT environments do not always have the right cybersecurity controls in their contracts. Hence, some systems remain unpatched and vulnerable to attack. Implementation of a risk-based integration/amalgamation approach is recommended. Assess the vulnerability of your current systems (OT, IIOT, IT) in the industrial environment, amalgamate only the necessary ones with patching, enable stringent third-party risk management with tight contractual controls and secure the industrial network with next-gen firewall security (integrated with Zero trust).

5. **Build next-gen identity and access management (IAM) and endpoint threat protection.** As the world moves to a mobile-driven approach, the importance of IAM and next-gen endpoint threat protection has grown exponentially. The complex nature of cyberattacks indicates that traditional forms of security – including tools such as antivirus and firewalls – will not be sufficient protection. The COVID-19 pandemic has further complicated this scenario as a major part of the workforce is now operating outside the perimeter of the secure enterprise network. Remote patient monitoring and DCTs have led to an increase in the number of unsecured devices and increased usage of technologies such as VPN to connect to networks, which makes visibility across the endpoint/device landscape difficult. Moreover, the combination of

Figure 3: Global Security Spend Per User, 2019-2020



Source: ISG Research 2021

legacy technology and an explosion of internet-facing endpoints and services are creating a new degree of complexity, which leads to configuration errors. Companies need to implement zero-trust architecture and least-access privilege and tightly controlled admin accounts. This should include continuous, password less and biometric authentication, advanced endpoint protection with artificial intelligence (AI), machine learning (ML) and behavioral analysis to correlate information and identify and remediate potential threats before they inflict damage.

Healthcare and Life Sciences organizations will undoubtedly remain key targets for cybersecurity threats, including large cyber espionage in years to come. Enterprise cybersecurity spend will continue to grow to bolster security standards and processes in these organizations. In addition to increased investment, companies must also continue to prioritize security throughout their transformation efforts.

ABOUT THE AUTHOR

Cybersecurity in Life Sciences in the Time of War and Pandemic: 5 Ways to Mitigate Risk

SAMEER NANDA

Director – Life Sciences, DACH

Sameer has more than 20 years of experience in Life Sciences industry. He has deep Life Sciences domain experience with a proven track record of leading and managing large, global multi-cultural teams to deliver complex digital transformation. In his focused career in Life Sciences, he has worked extensively in US, Europe and APAC region with global pharmaceutical clients as a trusted advisor for critical transformational initiatives. He has keen interest in – advanced analytics/BI, automation in Life Sciences industry, digital health strategy/transformation, patient engagement and architecture/strategy around – Master Data Management, promotional compliance, medical affairs, close loop marketing and remote patient engagement.

ABOUT THE AUTHOR

Cybersecurity in Life Sciences in the Time of War and Pandemic: 5 Ways to Mitigate Risk

ALOK TRIPATHI

Principal Consultant, DACH

Alok works as a Consulting Manager at ISG with 9+ years of experience in developing Cyber Security Strategy, assessing Cyber Security posture against various frameworks (CSA, NIST, etc.), development and implementation of IT Controls to ensure compliance standards (C5, ISO, etc.), experience with Cloud (private/public) security capabilities and solutions. He also has a good understanding of various cloud security configurations, technologies and frameworks.

ISG®

ABOUT ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, www.isg-one.com.

Let's connect NOW...