Guidehouse

**Life Sciences**

# From Cozy Bear, Lazarus Group, and Cerium, to FireEye and SolarWinds: Why Life Sciences Companies Require a Comprehensive Approach to Defend Against Cyberattacks

Life Sciences companies collect, store, and utilize large quantities of personal data, including personal health information related to drug trials, through Software as a Medical Device and digital therapeutics, and intellectual property, including innovative research (e.g., COVID-19 vaccine research), and other industry-specific technologies. This data is very attractive to cyber criminals, nation state-sponsored hackers, and competitors owned by countries. The consequences of a successful data breach can include the theft of intellectual property, compromised research data, lost revenue, and financial penalties.

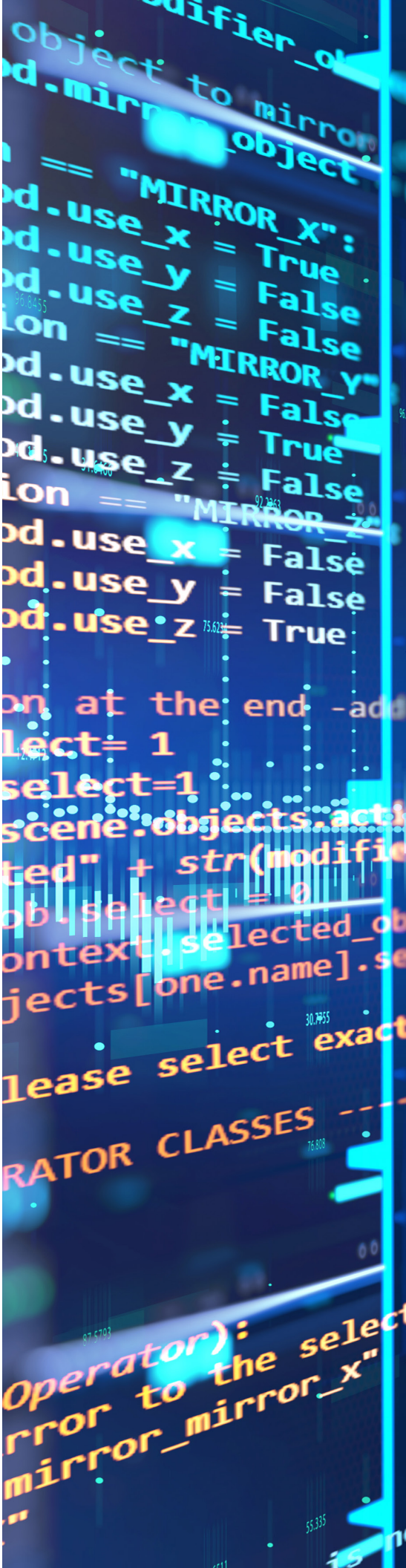
On March 2, 2021, Microsoft announced that zero-day vulnerabilities in its Exchange Server email and calendar software have been exploited by a Chinese hacking group it calls HAFNIUM. A variety of Microsoft clients were targeted including infectious disease researchers.[1]

A BBC News bulletin issued February 16, 2021, claims that North Korea attempted to steal COVID-19 vaccine technology from US Life Sciences company Pfizer, according to South Korean intelligence officials.[2]

In July 2020, APT29 (Cozy Bear) was identified by cybersecurity agencies from the UK, Canada, and the US as targeting pharmaceutical companies and academic institutions tied to COVID-19 vaccine development.[3]

A November 2020 media report states that Russia's APT28 (Fancy Bear), the Lazarus Group from North Korea, and another North Korea-linked group dubbed Cerium, are actively attempting to hack companies involved in COVID-19 vaccine and treatment research.[4]

AstraZeneca COVID-19 research was targeted by North Korea using fraudulent recruiting schemes to trick personnel into applying for fictitious job postings via LinkedIn and WhatsApp.[5]




1. Fox Business, "Microsoft says Chinese hackers targeted groups via server software," March 2, 2021, https://www.foxbusiness.com/technology/microsoft-says-chinese-hackers-targeted-groups-via-server-software.
2. BBC News, "North Korea accused of hacking Pfizer for Covid-19 vaccine data," February 16, 2021, https://www.bbc.com/news/technology-56084575.
3. Tara Seals, "Nation-State Attackers Actively Target COVID-19 Vaccine-Makers," Threat Post, November 13, 2020, https://threatpost.com/russia-north-korea-attacking-covid-19-vaccine-makers/161205/.
4. AP and Los Angeles Times, "Britain, U.S., Canada accuse Russia of hacking coronavirus vaccine trials," July 16, 2020, https://www.latimes.com/world-nation/story/2020-07-16/uk-us-canada-accuse-russia-of-hacking-virus-vaccine-trials.
5. Angus Liu, "AstraZeneca staffers targeted in suspected hacking scheme amid work on COVID-19 vaccine: report," Fierce Pharma, November 30, 2020, https://www.fiercepharma.com/pharma/astrazeneca-staffers-targeted-suspected-hacking-amid-work-covid-vaccine-report.

The SolarWinds Orion supply chain compromise in December 2020, led to cyberattacks against nine US government agencies and 100 private companies, including Procter & Gamble.[6] FireEye was the first company to discover the Solar Winds compromise.

As a highly regulated industry, Life Sciences companies are familiar with establishing and implementing internal controls and quality systems. However, these basic measures alone are not adequate to protect Life Sciences companies from the attackers that target them. A holistic program must be implemented to provide higher levels of protection and the cybersecurity program should include at least the following eight elements.

1. **Evaluate Current Cyber Hygiene Practices**

- **Ensure you know what data and systems are most critical to maintaining your organization's business and operations.** You should have a thorough and complete inventory of your most critical assets and know where your organization's most valuable data resides within the environment.
- **Assess your current cyber practices against the appropriate standards** for your organization—including National Institute of Standards and Technology, Center for Internet Security (CIS), International Organization for Standardization (ISO), and others—for vulnerability management, patch management, identity and access management, and configuration management.
- **Understand your external interconnections** and who you have allowed to access your systems (both IT and Operational technology) and whose technology you're using. This will help you better understand the risk to your organization and how these risks are being addressed. The existence of a security weakness in a business partner or vendor environment makes you vulnerable too.
- **Know the data that you share** with third-party business partners and vendors. Know how it is shared, how it is protected, and how its protection can be validated.

2. **Cyber Resilience—**Develop a strategy to build an environment to ensure your most valued data, operations, and business mission are the focus of the program. Consider network segmentation and restricting both internet exposure and third-party access. Create a baseline of your environment and consider tools that will help you monitor for anomalies.
3. **IT Strategy—**Develop and assess courses of action and strategies that define the future, enable transformation and modernization, increase performance, and improve services for your customers.
4. **Supply Chain Risk Management (SCRM)—**Engage your organization to develop an SCRM program to illuminate and identify risks to products, tools, and vendors.
5. **Enterprise Risk Management (ERM)—**Apply a risk-based approach to managing the security of your environment. Risks associated with data breaches should be evaluated against enterprise objectives and should consider enterprise strategies and risks. Include your Chief Risk Officer and engage support to help you prioritize your resources toward your most critical business risks.
6. **Cybersecurity —** Develop a comprehensive cybersecurity program to address gaps identified during the evaluation of your current practices. Ensure best practices are implemented and a sufficient governance structure is put in place. This should include an ongoing security awareness and training program focused on creating a cyber-conscious culture. The cybersecurity program should also address vulnerability management, patch management, identity and access management, least privilege, configuration management, data encryption, and email filtering.
7. **Regulatory Compliance Review—**Work with your legal department to ensure your reporting obligations are identified and up to date. Also consider international regulations If your organization conducts business internationally.
8. **Incident Response Training—**Invest in security incident response training and planning to ensure you can rapidly respond to and recover from a cyber incident, to include such things as a supply chain exploitation.

The Chief Information Officer and Chief Information Security Officer can no longer have sole responsibility for data protection. A robust governance model must be implemented and include participation from a broad range of stakeholders, including the Chief Financial Officer, Chief Risk Officer, Office of General Counsel, Human Resources, Corporate Communications, and Mergers and Acquisitions. A comprehensive risk management-based cybersecurity program combined with a robust governance model are required to adequately protect your organization against cyberattacks and the risk of value and reputational erosion that comes with this threat.

6. Laura Hautala, "SolarWinds not the only company used to hack targets, tech execs say at hearing," CNET, February 24, 2021, https://www.cnet.com/news/solarwinds-not-the-only-company-used-to-hack-targets-tech-execs-say-at-hearing/.

## Contacts

**Jack O'Meara**
Director, Cybersecurity Solutions
jomeara@guidehouse.com

**David Weiss**
Partner, Life Sciences
david.weiss@guidehouse.com

linkedin.com/showcase/guidehouse-health

twitter.com/GuidehouseHC