WHITE PAPER

Cybersecurity for the Life Sciences R&D Ecosystem

Kalleid JUS1ONE SECURITY

CONTENTS:

Cybersecurity for the Life Sciences R&D Ecosystem

The rate of data generation is increasing exponentially in today's technology driven world. This is especially true for R&D activities in the life sciences, where technologies like next generation sequencing (NGS) are creating terabytes of genomics data in a single run. Researchers in pharmaceutical and biotech companies typically work with massive repositories of research, clinical trial, and patient data to help identify and optimize potential new drug candidates, generating proprietary intellectual property (IP) in the process.

Large amounts of sensitive data and valuable IP make biotech and pharmaceutical companies prime targets for cybercriminals. While you can change your credit card number, you cannot change your DNA. Personal health and/or genomics data is thus very valuable and sought after by hackers, with electronic health records sometimes going for over $1000 on the dark web.[1] But it is not just external threats from hackers or malware that life science companies face, there can also be serious internal threats from disgruntled, noncompliant and/or malicious employees.

"Large amounts of sensitive data and valuable IP make biotech and pharmaceutical companies prime targets for cybercriminals. While you can change your credit card number, you cannot change your DNA."

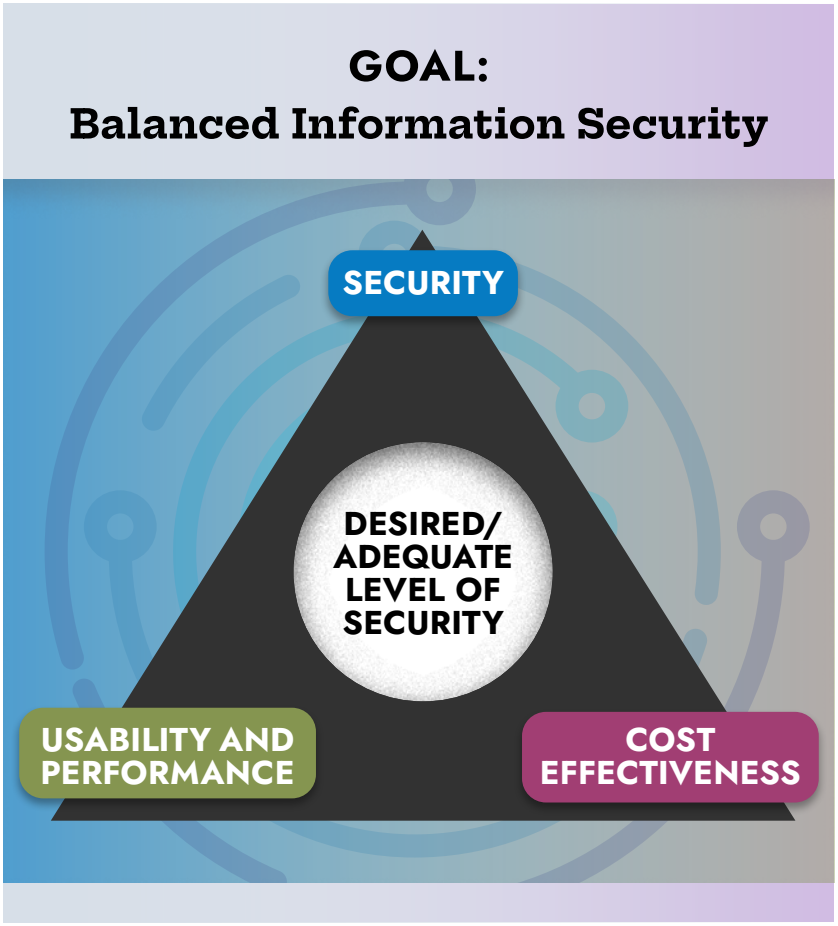
The first high-profile cyberattack against a pharmaceutical company came in 2017, with the NotPetya ransomware attack, which was perpetrated by state-sponsored hackers. While the NotPetya malware affected companies around the world, it hit the global drug maker Merck particularly hard, crippling more than 30,000 laptop and desktop computers, along with 7,500 servers. NotPetya malware locked up critical Merck files via encryption, with the hackers promising to release the files for $300 in bitcoin per affected computer. Unfortunately, the malicious malware damaged files beyond repair in the process of encrypting them. All told, the NotPetya ransomware attack cost Merck an estimated $870 million in revenue in 2017 alone.[2]

Since 2017, cyberattacks on pharmaceutical and biotech companies have been on the rise. A report by the cybersecurity firm BlueVoyant reveals that publicly declared cyberattacks on the biotech and pharmaceutical industry jumped by 200% in 2018, and another 50% in 2019.[3] This past year (2020) has seen aggressive and focused hacking attempts by nation-state actors on pharmaceutical companies pursuing COVID-19 vaccines and treatments. The COVID-inspired remote work trend has provided a promising attack vector for hackers seeking to exploit vulnerabilities in remote connections. As noted in the BlueVoyant report, of the 25 cyberattacks on the pharmaceutical and biotech companies reported to the media since 2017, 40% took place in 2020.

- In April 2020, Iran-linked hackers targeted Gilead Sciences staff.[4]
- In May 2020, the FBI and the US Cybersecurity and Infrastructure Security Agency (CISA) issued a warning to organizations researching COVID-19 of "likely targeting and network compromise" by China.[5]
- In July 2020, developers of Covid-19 vaccines were targeted by a Russian hacking group known as APT29.[6]

Due to the serious nature of the threat, most pharmaceutical organizations have been significantly ramping up their investment in good cybersecurity for their own systems. One area that is often overlooked, however, is the security capabilities and practices of all the collaborators in the greater research ecosystem that have access to (and thus provide a backdoor into) the research sponsor's sensitive data.

Hackers look for weak points in a network, and many of the smaller research collaborators in the greater pharma research ecosystem (e.g., Universities, research hospitals, teaching hospitals, etc.) have notable gaps in their cybersecurity practices and systems. In today's cyber threat environment with sophisticated, well resourced, and relentless hackers, a single breach in a pharma research network can have catastrophic consequences.



Unfortunately, many companies are behind the curve on this threat. A recent survey by BlueVoyant of 301 CIOs, CISOs and CPOs in the United States found that 92% of respondents suffered a breach at the hands of a third party in last 12 months, while 69% revealed that they had limited visibility into their 3rd party vendors.[7] Over a quarter (27%) of the respondents reported that they only reassess and report on third-party cyber risk six monthly or less frequently, meaning they spend at least half a year with no insight into the changing risk in their supply chain and/or collaborator network.

Despite cybersecurity investment by major biopharmaceutical companies being on the rise, CIOs and CISOs are experiencing multiple pain points in operationalizing their cyber risk management across a vast research network that often includes collaborators in emerging markets. The life science industry has a need for an effective cybersecurity approach that serves to facilitate secure, productive and cost-effective collaboration in drug discovery research.

In this white paper, we will propose a risk-based security framework that fulfills this need based on the model used by the grant issuing agency of the NIH. We will also provide a case study where this model was successfully applied for a global pharmaceutical organization.

Cybersecurity Standards Within the Federal Government

Life Science companies seek to create a research ecosystem that is both productive, cost-effective, and secure using a variety of third-party collaborators to store, manage, process and even create data. Credit card companies mandate adherence to the Payment Card Industry Data Security Standards (PCI DSS) by merchants to ensure the security of credit card transactions.[8] In the life science industry, however, there is no official security standard that would serve to expedite the assessment of potential research partners for pharmaceutical companies.

When sharing research data with a collaborator, pharmaceutical companies need to confirm that the partner has an acceptable level of security practices to protect sensitive research data both in transit and when it arrives at its destination. To obtain the necessary assurance before moving forward with data sharing, pharma companies often send out a survey with hundreds of questions to a potential collaborator to assess their security practices. For obvious reasons, this evaluation method is cumbersome, time-consuming, and subjective.

A proposed solution to this problem, for both the pharma company and the third-party collaborator, is to apply federal cybersecurity standards that are well documented and can be tailored to fit the pharmaceutical research ecosystem. Towards this end, the Federal Information Security Management Act (FISMA) defines the appropriate extent of security controls and measures commensurate with the risk and potential damage done by the unauthorized use, destruction, theft, or sequestering of federal agency data.[9]

FISMA gave National Institutes of Standards and Technology (NIST) the ability to set security requirements to ensure the safe harbor and transfer of protected federal information. The risk-based, flexible approach of the NIST framework makes it particularly well-suited for a research environment. Currently, the NIST security requirements are applied to all branches of the military and federal agencies, including the grant issuing agency of the NIH. The requirements are implemented to ensure the security of information in the following categories:

- **Confidentiality** – "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."
- **Integrity** – "Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity."
- **Availability** – "Ensuring timely and reliable access to and use of information."

The NIST Risk Management Framework (RMF)

In a typical pharma research ecosystem, there is a central research IT group that effectively functions as a managed service provider for many different collaborating labs, all of which have different data security needs based on the type of work they are doing and the data they are handling. A collaborator's risk profile can range from very low (e.g., doing research on low risk or model organisms) all the way up to high (e.g., clinical research where you are handling genetic profiles of patients).

NIST Risk Management Framework

Step by step overview

Identify Assets: This first step focuses on identifying information and system assets and determining how they align with your organizational risk management strategy. Using guides in federal publications, organizations assess the impact of critical data security failures in terms of confidentiality, integrity and availability and assign the appropriate risk category using a Low, Moderate, High scale.

Select Controls: Based on the risk level identified, security requirements are then selected from the NIST special publications. There are templates for each level — Low, Moderate, and High. These templates take the guesswork out of the selection process.

Implement Controls: In this step, the risk-based security program is implemented. While policies and procedures apply to all systems, technical controls may be tailored to an individual information system based on the relevant security risk level that has been identified. For research organizations, this has a significant impact on cloud-based projects.

Assess Controls: Implemented controls are examined to verify effectiveness in what they're intended to protect. To build more trustworthiness, organizations can have an external provider perform a 3rd party assessment of the controls. These types of assessments are commonplace and are required for most business to business collaborations.

Authorize the System:
The information system must be accepted by the executive that is ultimately responsible for it. This acceptance is an official recognition that the system meets or exceeds the security expectations put forth in the risk management strategy applied in Step 1.

Monitor the System: Shortly after a security program is established, it will become dated. In order to maintain an effective and sustainable program, an operational plan must be developed and followed. Policies, procedures, and technical controls must all be updated to keep up with threats and trends in research and development.

It doesn't make sense from a cost or operational perspective for the central research IT group to apply the same stringent security standards to everyone in the network. They simply don't have the capability to manage and/or embed resources in every single lab or collaborator that needs to be managed. What the managing IT group needs is a risk-based template that enables them to manage security for a variety of systems effectively under one roof with just a few people.

Similarly, scientists doing low risk discovery activities want to maximize data sharing and collaboration without being burdened with stringent security checklists that slow down their research. These researchers want appropriate security standards to be applied in ways that do not unnecessarily hamper their discovery work.

To address these needs in the context of the federal government, NIST developed a 6-step process (see infographic) called the Risk Management Framework (RMF).[10] The grant issuing agency of the NIH has a small security team that applies this framework to manage security for the many different institutes and constituents that they work with. The RMF is tailored to meet the requirements of confidentiality, integrity, and availability (CIA) based on the assessed risk of each organization in the network.

The risk-based approach of the NIST RMF provides an effective data security template that could be applied to a pharmaceutical research ecosystem to fulfill the needs of the central research IT group, the collaborating organizations, and the scientists doing the research. That said, organizations within the ecosystem would not necessarily follow RMF exactly as it is written. The idea is to use the RMF as a guide, while aspiring to not stray too far from it.

With pharmaceutical companies increasingly relying on external collaborators as a critical component of their innovation engine, trying to prevent every possible incident is simply not realistic from a cost perspective. While greater investment may be required from pharmaceutical organizations to prevent a serious breach, it is important to invest in a risk-based fashion. The NIST RMF helps define the organization's top risk areas and assets and model realistic attack scenarios, enabling a reasonable level of investment in a quality cyber risk program.

Customized Security Plans for Pharmaceutical Companies and Collaborators

While some organizations in the pharma research ecosystem may want to pursue a comprehensive RMF approach, which can include NIST audits and internal certification, others may have less aggressive goals. For example, an organization that is interested in becoming a more attractive and/or trustworthy partner for a pharmaceutical sponsor or a grant issuing agency like the NIH may be interested in adopting the Risk Management Framework. Some collaborators may be interested in an RMF program only for high-risk systems, while others may build a program for the entire organization. On the other hand, an organization that is simply interested in shoring up the security of operations may just want to increase researcher awareness of the security systems in place with a comprehensive training program.

By employing a risk-based methodology, along with the right processes and technologies, organizations can secure their research data and maintain a high-level of productivity in their discovery activities to fuel innovation. Towards this end, it is important to work with a 3rd party consultant who understands the RMF template and can create a customizable security program based on the customer's needs and objectives. A quality security consultant can help research IT organizations and their collaborators have a better understanding and control of their environment, along with a more directed and informed investment of resources.

Organizations can secure their research data and maintain a high-level of productivity in their discovery activities to fuel innovation.

In order to gain a better understanding of how the NIST RMF can benefit your organization, let's take a look at a case study where it was utilized successfully in the context of a comprehensive cancer center and research institute.

CASE STUDY:

Implementing RMF Compliant Security for a Cancer Research Institute

OVERVIEW

The research arm of a comprehensive cancer center was working with the NIH to conduct clinical trials in cancer research. In order to optimize its research efficiency, the center embarked on a digital transformation project to place all technology assets in the cloud and provide open-source access to the base code.

Given potential security risks inherent in moving to the cloud, the NIH grant issuing agency ruled that the project had to fall under their security policy structure which follows the federal FISMA guidelines using the NIST risk management framework (RMF).

The research arm of the cancer center was still in the early stages of its cloud strategy and did not have a mature security model that was a good fit for this infrastructure upgrade. Unfamiliar with the RMF and the federal security assessment process, the research team reached out for help from a security consultant.

SERVICES PROVIDED

The security consultant was hired to be a subject matter expert, facilitator, and advocate in the process of implementing the RMF for the cloud migration project. The consultant served as an effective guide for the project's leadership in the implementation of policies, technologies, and processes that would put them in compliance with their RMF security goals, while at the same time maintaining the agility required by a research team.

Key services provided by the consultant included:

- **Security Assessment** – The consultant conducted a current capabilities assessment in order to determine the gap between current practices and those required by the RMF for base-level compliance. Upon project initiation, there were no formal translatable NIST policies or procedures.
- **Project Plan** – The consultant developed a project plan that would include the steps needed to be taken to develop a complete NIST RMF compliant security program. This plan included all of the controls, policies, procedures and workflows necessary for compliance.
- **Security Program Development and Support** – The consultant authored the security policies, and, with close collaboration with the research and technology teams, supported the development of compliant procedures and workflows that align with the research objectives of the project.
- **Information Security Training** – The consultant managed the education profile of the project's user space by access level and developed the team's OWASP training materials for administrators.
- **Security Point of Contact** – To alleviate the management burden of program oversight, the consultant served as a point of contact for all services related to vulnerability assessment, security risk assessments, and audits. The consultant aggregated and educated the project team on what to expect and how to comply with an audit for success.
- **Research Tailored** - Utilizing extensive knowledge in molecular biology, genetics, and the technologies supporting biomedical research, the consultant was able to provide important perspective regarding security control implementation that helped balance the often-competing needs of researchers and security. The consultant effectively advocated for critical research processes and developed compensating options for security controls to satisfy requirements.

RESULTS DELIVERED

The consultant worked with the cancer center in the first year to reach a NIST RMF-Low compliance standard. With this compliance standard achieved, the project successfully attained a risk acceptance memo from the NIH, which enabled the project to proceed in pilot phase while working on attaining an RMF-moderate compliance standard the following fiscal year.

In year two, the project was audited for RMF-moderate compliance by a third party, assessed for residual risk, and ultimately attained their authority to proceed from the NIH. With this designation of a third party certified, federally secure system, the project is able to proceed into operational capacity and begin their three-year cycle of RMF recertification.

Conclusion

Drug discovery activities in the life sciences is a highly data-driven and collaborative process. Secure and productive data sharing in health research is essential to fuel the innovation pipeline, yet the need to continuously protect all forms of data in all locations and transmissions can be a challenging task. This is especially the case in industry-leading organizations striving to integrate legacy systems and digitize all aspects of the product lifecycle in order to gain a competitive advantage.

With sophisticated and targeted cyberattacks against biotech and pharmaceutical companies on the rise, managing collaborator cybersecurity risk in the burgeoning pharma research ecosystem is rapidly becoming the dominant cybersecurity challenge for life science companies. As pharma companies have increased the number and variety of collaborators they work with in the pursuit of competitive advantage, they have inadvertently exposed their enterprise network to the vulnerabilities of those partners.

While scientists in the pharma research ecosystem want full control of their data to enhance their research through collaborations with colleagues and organizations, security teams have the challenge of protecting information from unauthorized use and disclosure. Business executives, on the other hand, all too often fail to make the connection between cybersecurity and business value.

The interface between research, security, and business leaders within life science organizations is often plagued with dysfunction fueled by gaps in communication and understanding between these groups. A quality security consultant fluent in the languages and needs of researchers, research technologies, and cybersecurity can bridge the gaps between these different stakeholders and establish a manageable cybersecurity program that is effective, comprehensible, and complimentary to the field of research and development.

In this white paper, we presented a risk-based cybersecurity framework (NIST RMF) for the life science industry that that aligns with federal grant agencies and is tailored to support the needs of researchers. Whether applied to a single system or a multi-cloud environment, the program scales as needed, is cost-effective, can be managed by a small team, and serves to facilitate secure and productive collaboration in health research. This model allows research organizations to maintain high levels of productivity, ultimately helping to facilitate the innovative research that delivers life-changing medications to patients in need.

About Kalleid: Kalleid, Inc. is a boutique IT consulting firm that has served the scientific community since 2014. We work across the value chain in R&D, clinical and quality areas to deliver support services for software implementations in highly complex, multi-site organizations. We pride ourselves in supporting the success of your IT projects and overall organizational transformation efforts with a wide range of interconnected services. At Kalleid, we understand that cybersecurity is a critical concern for research organizations, and we work with our partner network to deliver customizable security plans that are aligned with our client's goals. For more information, visit **kalleid.com.**

About Just One Security: Just One Security professionals are well-versed in the language of cybersecurity, IT and life science research. Using our diverse experience and PhD level expertise in biomedical research, informatics, cloud technologies, IT architecture, data security, and the RMF, we build positive relationships with our clients to streamline and facilitate the implementation of security practice. Our central calling is to deliver manageable cybersecurity programs that are effective, comprehensible, and complimentary to the field of research and development, saving our clients time and resources. For more information, visit **justonesecurity.com**

[1]"Your Electronic Medical Records Could be Worth $1000 to Hackers," Forbes, Apr 14th, 2017. Mariya Yao. Available at: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/?sh=78d8568f50cf

[2]"Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead – sources," Reuters, May 8th, 2020. Jack Stubbs et al. Available at: https://www.reuters.com/article/us-health-care-coronavirus-gilead-iran-ex-idUSKBN22K2EV

[3]"FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations," FBI Press Release, May 13th, 2020. Available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-and-cisa-warn-against-chinese-targeting-of-covid-19-research-organizations

[4]"Russian Hackers Launch Cyber Attack on Covid-19 Vaccine Developers," Labiotech, July 7th, 2020. Available at: https://www.labiotech.eu/medical/covid-19-vaccine-cyber-attack/

[5]"Global Insights: Supply Chain Cyber Risk," BlueVoyant, September 2020. Available at: https://www.bluevoyant.com/ciso-report-download-form

[6]"PCI Compliance," Investopedia, April 20, 2020. Julia Kagan. Available at: https://www.investopedia.com/terms/p/pci-compliance.asp

[7]Wikipedia Page. Available at: https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

[8]"Risk Management Framework," NIST. Available at: https://www.nist.gov/cyberframework/risk-management-framework