Illumina

Cybersecurity Assessment

Date: April 14th, 2024

Team Members: [redacted], [redacted], and Emma Humphreys

Table of Contents

Company Profile

Company Description

Illumina, headquartered in San Diego, California, is a pioneering biotechnology company that has been at the forefront of genomic research and DNA sequencing since its founding in 1998. Renowned for its cutting-edge sequencing platforms, including NovaSeq, HiSeq, and MiSeq systems, Illumina has significantly advanced the field with its innovative sequencing-by-synthesis technology. The company's comprehensive range of products encompasses sequencing instruments, reagents, and software solutions, addressing diverse genomics applications such as whole-genome sequencing, targeted sequencing, and gene expression analysis. Illumina's commitment to innovation has contributed to the widespread adoption of genomic technologies globally, impacting scientific research, clinical diagnostics, and personalized medicine. With a strong global presence, Illumina actively collaborates with academic institutions, pharmaceutical companies, and other organizations to expand the applications of genomics. In addition to its products, Illumina provides sequencing services, allowing researchers and organizations to leverage the company's expertise and infrastructure for outsourced sequencing projects. Illumina's transformative contributions continue to shape the landscape of genomics, making it a key player in the biotechnology industry. The company also has a strong belief in the power of genome development, as they claim that it can cure many diseases and even extend human lifespan. On their about page, they emphasize their mission is not just to offer a solution through gene therapy, but to also make it flexible, scalable, and supported with industry-leading services, ensuring global accessibility beyond affluent nations.

Company History

Founded in April 1998 by David Walt, Larry Bock, John Stuelpnagel, Anthony Czarnik, and Mark Chee, Illumina quickly emerged as a leader in genetic sequencing and array technologies. While initially incubated at Tufts University in Massachusetts under the CW Group venture capital firm, they swiftly licensed their prototype BeadArray technology. By July 2000, the company had relocated its headquarters to San Diego, California, and completed its initial public offering on the stock exchange. Throughout the early 2000s, Illumina remained dedicated to technological advancement, introducing innovations like single-nucleotide polymorphism (SNP) analysis in 2001 and GoldenGate Genotyping technology by 2002, culminating in the launch of their BeadLab system. Their technologies gained global traction, embraced by academia, governments, and biotech institutions worldwide.

In January 2007, Illumina acquired Solexa, further expanding its genetic analysis capabilities to encompass gene and RNA analysis. By 2009, Illumina announced the launch of personal full genome sequencing services, albeit at a hefty price of $48,000 per genome. However, rapid advancements drove costs down significantly, with prices plummeting to $4,000 per genome in 2012 and further to $1,000 per genome today. Illumina's trajectory intertwined with strategic acquisitions like Solexa and GRAIL, strengthening its position in the biotech landscape. The company's legacy includes pioneering breakthroughs such as the BeadArray technology in 2001 and the development of leading

sequencing platforms like the Genome Analyzer and HiSeq systems. Their expansion into clinical diagnostics, with platforms like MiSeqDx and NextSeq 550Dx, garnered regulatory approvals and extended their impact into cancer genomics, rare disease diagnosis, and population genetics. Continual innovation in sequencing chemistry and data analysis tools underscores Illumina's ongoing influence on scientific discovery and healthcare applications.

About the Industry

The bio-genetic industry, located at the nexus of biology and genetics, involves diverse stakeholders crucial to its dynamic evolution. In the transformative field of genomics, scientists and researchers explore genomes using technologies like high-throughput sequencing to decipher genetic information. Biotech companies translate these genomics discoveries into therapies and genetically modified products, while governments and regulatory bodies shape policies for ethical and safe applications. Ethicists and social scientists examine the profound implications of genetic manipulation, and patients/consumers navigate the transformative landscape of personalized medicine. Collaboration among researchers, companies, regulators, ethicists, and consumers is essential in addressing the multifaceted challenges and opportunities inherent in the bio-genetic industry, driving innovations in diagnostics, therapeutics, and our fundamental understanding of the genetic code.
Illumina stands at the forefront of not one, but two pivotal arenas within the gene therapy landscape: research and medical devices. Delving deep into the realms of research, the company's dedicated teams tirelessly investigate the transformative potential of genetic modifications in combating the formidable challenges posed by cancers and other diseases that have long eluded conventional medical interventions. Simultaneously, within the domain of medical devices, Illumina collaborates closely with its esteemed subsidiary, Solexa, to engineer cutting-edge devices meticulously designed to dissect and analyze genes and DNA with unparalleled precision. This symbiotic partnership has empowered Illumina to forge ahead, pioneering the development of exceptionally precise methodologies in disease treatment within their esteemed research department. Regarded as the vanguards of the gene therapy movement, Illumina's groundbreaking contributions continue to shape and redefine the trajectory of genetic medicine on a global scale.

Key Products

Illumina's remarkable portfolio in the gene therapy field is anchored by their iconic creation, the BeadLab, which has remained a pinnacle of their innovation since its inception in 2002. This groundbreaking device boasts the capability to target or conduct whole genotyping of human samples, facilitating precise medical research and propelling Illumina to the forefront of gene therapy advancements. Inspired by the BeadLab's success, subsequent technologies, such as the genome analyzer, have emerged, enabling even more precise genome readings and catalyzing breakthroughs in gene development technology. Additionally, AmpliSeq stands as a testament to Illumina's commitment to excellence, providing sequencing solutions that enhance accuracy alongside their proprietary gene sequencing platforms, further solidifying their position as leaders in the field.

Beyond individual products, Illumina's comprehensive range encompasses sequencing instruments, reagents, and software solutions, addressing diverse genomics applications spanning from whole-genome sequencing to targeted sequencing and gene expression analysis. Their unwavering dedication to innovation has not only fueled the widespread adoption of genomic technologies worldwide but has also significantly impacted scientific research, clinical diagnostics, and personalized medicine. Moreover, by offering sequencing services, Illumina extends its expertise and infrastructure to researchers and organizations, facilitating outsourced sequencing projects and further shaping the landscape of genomics. Illumina's transformative contributions underscore its pivotal role in the biotechnology industry, marking it as a key player driving advancements in the realm of genetic medicine.

Introduction

This paper explores the cybersecurity risk assessment at Illumina, a leading genomics company, highlighting vulnerabilities in its systems and proposing comprehensive strategies to combat potential cyber-breaches. By analyzing the evolving threat landscape and assessing Illumina's current security posture, it is evident that proactive measures are imperative to safeguard sensitive genomic data. Recommendations include implementing robust encryption protocols, enhancing employee training, establishing incident response plans, and fostering collaborations with cybersecurity experts. By prioritizing cybersecurity initiatives, Illumina can fortify its defenses and maintain public trust in its critical genomic research endeavor.

Asset Ranking

Key Assets			
Digital Asset	**Description**	**Value (1 - 19) (1 being highest priority)**	**Explanation/Reasoning**
Point of Sale (POS) System	Illumina sells genomic sequencing kits, and software on its website. As such, they have a POS system for customers to pay for these items.	19	If Illumina's POS system were to be hacked the company would lose significant revenue; and could have their reputation damage if customers were still able to make purchases before the company realized their POS was taken over by a hacker.
Illumina Connected Analytics (ICA)	Illumina Connected Analytics (ICA) is a secure, cloud-based genomic data platform that Illumina uses for analytical purposes.	6	If this platform were to be hacked, or otherwise tampered with (either from external or internal means) it could mean data is lost, stolen, misused, or tampered with. It could also open them up for suits from clients who's genetic sequencing they keep in cloud-based systems.
Sequencing Platforms/ Services	Illumina offers several next-generation sequencing (NGS) services.	5	Illumina must be cautious of the networks these services are performed on to ensure the only those who are authorized to have access are able to view the data used for these services.
Emedgene Analysis Platform	Illumina Emedgene Analysis Platform is a service that provides analysis of genetic sequences for rare genetic diseases.	7	Illumina should be aware of the security protocols around maintaining data (just like other genetic information); however, due to the nature of the genetic diseases studied using this platform, Illumina should take additional precautions in maintain the security of these diseases to ensure that the data is not tampered with or used in a malicious way.
Illumina Proactive Instrument Performance Service	Illumina Proactive Instrument Performance Service is an additional offering customers can purchase when buying an instrument or software from Illumina. This is a remote service where engineers can 'remote' in and provide maintenance advice/ service the product.	8	Due to the 'remote-in' nature of this service, Illumina and the client must make sure that the connection is secure. If there is a vulnerability with either party involved in the connection a hacker could join and breech the system.
Customer Genomic Data/ Genomic Data Repositories	Digital repositories and databases play a pivotal role in modern genomic research, housing curated genomic datasets and reference genomes essential for in-depth analysis and investigation. Illumina, as a leading genomic sequencing company, offers a suite of analytic platforms, genetic sequencing test kits, and advanced sequencing software. During their operations, Illumina frequently maintains and accesses customer genetic information.	1	Genomic data repositories serve as invaluable assets for researchers, facilitating data sharing, collaboration, and the comparative analysis of genomic findings. However, if Illumina's stored genetic data is not properly secured, it becomes susceptible to potential breaches by hackers. In the event of such a breach, stolen genetic data poses significant privacy and security risks, highlighting the critical need for robust data protection measures across the genomic landscape.
Bioinformatics Software Platform	Comprehensive software platform for processing, analyzing, and interpreting genetic data obtained from DNA sequencing.	3	Bioinformatics software is the backbone of Illumina's data analysis pipeline, enabling researchers to derive valuable insights from genomic data.
Cybersecurity Infrastructure	Network security systems, firewalls, intrusion detection/prevention systems, and encryption protocols protecting Illumina's digital assets and sensitive genetic data from cyber threats.	4	Cybersecurity infrastructure is crucial for safeguarding Illumina's digital ecosystem, preventing unauthorized access, data breaches, and cyberattacks.
Cloud Computing Services	Cloud-based storage and computing services for scalable and flexible data storage, processing, and analysis of genomic data.	9	Cloud computing services offer cost-effective and scalable solutions for managing Illumina's growing volumes of genomic data, enhancing accessibility and computational capabilities.
Laboratory Information Management System (LIMS)	Digital platform for managing laboratory workflows, sample tracking, and data management in genomic research and analysis.	13	LIMS facilitates efficient laboratory operations, ensuring accurate sample tracking, data integrity, and compliance with regulatory requirements.
Electronic Health Records (EHR) Integration	Integration of genomic data with electronic health records (EHR) systems for personalized medicine and clinical research.	10	Integrating genomic data with EHR systems enhances patient care, facilitates research on genetic diseases, and supports clinical decision-making.

Key Assets			
Digital Asset	**Description**	**Value (1 - 19) (1 being highest priority)**	**Explanation/Reasoning**
Research Collaboration Platforms	Digital platforms for collaboration, data sharing, and project management among researchers and partners in the genomics community.	11	Research collaboration platforms foster innovation, knowledge exchange, and interdisciplinary collaboration in genomics research and development.
Knowledge Management Systems	Digital systems for capturing, organizing, and sharing institutional knowledge, best practices, and research findings within Illumina.	12	Knowledge management systems facilitate knowledge sharing, collaboration, and innovation within Illumina's workforce, enhancing productivity and decision-making capabilities.
Research Labs and Scientists	Around the clock, dedicated researchers utilize labs to delve into genomes, aiming to unearth novel strategies for combating diseases such as cancer, Alzheimer's, dementia, and diabetes. Their tireless efforts drive innovation within the genetic sphere, fostering breakthroughs that hold promise for curing ailments and reshaping the landscape of medical science.	2	Without research labs and the scientists who work in them, foundational work on genomes would be impossible, hindering innovative breakthroughs and revenue generation for the company. These labs provide scientists with essential workspaces, crucial for conducting their research effectively. Neglecting these facilities would not only exacerbate the already stressful nature of scientific work but also impede progress due to inadequate conditions.
Illumina Operational Qualification	This is a qualification certificate that certifies the appointed to the Illumina instruments when they meet regulatory requirements. The instruments must go through testing and validation to make sure these instruments are within great/optimal performance.	15	I believe that out of every asset that this company has to offer this is most likely the least important. I believe that everything on this list is pivotal in studying genes and DNA/RNA strains, but this is just a certification for the instruments that they provide. While this is important, I believe that it is the least important when it comes to this list of assets. That is wh putting it at number ten.
Marketing and E-commerce	Online platforms for marketing Illumina's products and services, as well as facilitating e-commerce transactions for product purchases.	16	Digital marketing and e-commerce platforms expand Illumina's reach, engage customers, and drive sales of sequencing systems, reagents, and services.
Supply Chain	The chain of supplies used in making Illumina's genome sequencing products	17	If Illumina's supply chain is affected, and they are unable to get the components necessary to complete their devices the company would lose significant amounts of revenue.
Secured Communication	Illumina would need to implement secure methods of communication as they would be transferring PII and other sensitive information	18	If Illumina's methods of communication were to be hacked it could lead to customer's PII being leaked (email/ phone calls/ video chats). This information could be numerous malicious ways from simple identity theft to more complex hacks gathering data.

Risk Management Matrix

#	Related Asset	Risk Description (Examples only - Yours will be different)	Business Consequences	Severity (0 - 100)	Likelihood (0 - 100%)	Score (Severity * Likelihood)	Mitigation	Responsible	Accountable	Consulted	Informed
1	Point of Sale (POS) System	Malware	POS could be taken down/ offline by an attacker, and therefore would mean potential customers would not be able to make purchases.	60	75.00%	45	To protect its POS system Illumina should implement robust firewalls, and anti-virus software. They should also ensure that these mitigation tools are maintained properly, and updates/ patches are completed in a timely manner to prevent vulnerabilities.	Information Technology	Information Technology	Marketing	Sales
		Ransomware						Information Technology	Sales	Operations	Executive Team
2	Illumina Connected Analytics (ICA)	Denial of Service attacks (DoS) Ransomware Internal threat (inside hacker)	If Illumina were to lose access to their ICA platform through either a denial of service; ransomware.	90	85.00%	76.5	To mitigate risks presented by Illumina's ICA platform the company should implement stringent authentication measure for users to access the platform at login. It would be recommended that they utilize a two-factor authentication method, such as Duo. Further mitigation methods such as firewalls and separating the platform from the rest of the network would allow Illumina the ability to isolate it if someone were to gain access to a portion of their network to prevent further attacks.	Information Technology	Information Technology	Information Technology	Executive Team
3	Website	Denial of Service attacks (DoS)	If Illumina were to lose control over their website, it could impact their POS system-- depending on how sophisticated and	30	50.00%	15	To mitigate Illumina's website from being hacked or taken down they should ensure that there are proper firewalls, and security measure in place.	Information Technology	Operations	Marketing	Executive Team

#	Related Asset	Risk Description (Examples only - Yours will be different)	Business Consequences	Severity (0 - 100)	Likelihood (0 - 100%)	Score (Severity * Likelihood)	Mitigation	Responsible	Accountable	Consulted	Informed
			quickly the attack moved through the network.								
4	Customer Genomic Data/ Genomic Data Repositories	Ransomware Denial of Service attacks Internal threat	If Illumina were to lose their stored genomic data, it could result in catastrophe. The loss of this data would result in a damaged reputation, and potential lawsuits with financial implications.	95	86.00%	81.7	As a genomic research company that conducts analysis of customer's genetic sequencing Illumina stores vast quantities of sensitive data. If this data were to be leaked, or compromised it would result in loss of reputation, and potential legal action that could financially ruin the company. As such, Illumina should keep all genetic sequencing data separate, and isolated from the main network. This would slow-down, and possible remove the risk of a hacker being able to access this information if Illumina's main network were to be breached. It is also important from an information governance stance to understand where all this data is stored, so the company can alert the necessary individuals if a breach were to occur. Another important aspect of securing this data is ensuring that all employees have a good understanding of cyber-hygiene and have received the proper cybersecurity training. Illumina's IT department should also ensure that there is a protocol in place to remove user accounts that are no longer in use (terminated employee, etc.).	Information Technology	Operations	Information Technology	Executive Team

#	Related Asset	Risk Description (Examples only - Yours will be different)	Business Consequences	Severity (0 - 100)	Likelihood (0 - 100%)	Score (Severity * Likelihood)	Mitigation	Responsible	Accountable	Consulted	Informed
5	Supply Chain	Ransomware Malware Denial of Service attacks (DoS)	Manufacturing plants being taken offline/ shut down by ransomware/ malware. Potential loss of trade secrets (dependent on how individual parts are made)	50	50.00%	25	To prevent a cyberattack on their supply chain, Illumina should ensure that their component suppliers have the most up-to-date patches, and software running on their servers. Illumina should also understand the mitigation processes in place by their component suppliers. As a company Illumina should ensure that their firewalls are maintained, and ensure employees understand the importance of cyber-hygiene.	Information Technology	Operations	Information Technology	Executive Team
6	Bioinformatics Software Platform	Software Vulnerabilities		95	80.00%	76	Regular software updates and patches, security testing, and code reviews to identify and address vulnerabilities promptly.	Information Technology	Marketing	Marketing	Information Technology
7	Cybersecurity Infrastructure	Data Breach		95	60.00%	57	Implementation of advanced encryption protocols, regular security audits, employee training on cybersecurity best practices, and incident response planning.	Executive Team	Information Technology	Operations	Legal
8	Cloud Computing Services	Data Loss Due to Service Provider Failure		80	40.00%	32	Implementing backup and redundancy measures, selecting reputable and reliable cloud service providers, and contractual agreements ensuring data recovery and service continuity.	Information Technology	Information Technology	Operations	Executive Team
9	Laboratory Information Management System (LIMS)	System Downtime		80	60.00%	48	Regular maintenance, redundancy in critical components, and backup systems to minimize downtime. Additionally, implementing robust disaster recovery plans.	Information Technology	Marketing	Marketing	Marketing

Assessment Recommendations

Asset 1: Cloud Computing Services ([redacted])

Explanation: Cloud computing services are utilized by Illumina to store and process genetic data. However, they pose a significant risk of data breaches due to the sensitive nature of the stored information.

Risk Category/Sub-Category: Information Risk - Data Breach

Rationale: Securing Illumina's cloud computing services through encryption and continuous monitoring is essential for safeguarding genetic data against unauthorized access or breaches. Encryption ensures that data remains protected both at rest and in transit, while continuous monitoring enables timely detection and response to potential security threats or breaches. This proactive approach enhances data integrity and minimizes risks to Illumina's operations.

Recommended Control:

Protect

Illumina has instituted a comprehensive policy aimed at fortifying the security of genetic data within its cloud computing infrastructure through the implementation of robust encryption measures. This policy mandates that all genetic data stored and transmitted via cloud infrastructure must undergo encryption to uphold confidentiality and integrity. The primary objective of this policy is to mitigate the potential risks associated with data breaches and unauthorized access by imposing strict encryption requirements for genetic data within Illumina's cloud computing services. Encryption, regarded as a foundational security measure, effectively renders sensitive data indecipherable to unauthorized users, thus bolstering overall data protection. To ensure the effective implementation of this policy, Illumina will establish clear encryption standards and protocols that align with industry best practices. Integration of encryption mechanisms into the cloud infrastructure will be carefully orchestrated to encrypt data both at rest and during transmission. Additionally, routine assessments of encryption technologies will be conducted to uphold compliance and address emerging security threats promptly. Compliance verification mechanisms will be rigorously enforced to uphold the integrity of the encryption policy. Illumina will conduct regular audits of encryption implementation, supplemented by automated monitoring tools tasked with scrutinizing data transmissions to ensure consistent encryption application. Any deviations from the prescribed encryption standards will trigger immediate alerts, prompting swift investigation and remediation actions.

Detect

In alignment with its proactive security stance, Illumina has embraced a robust policy dedicated to the early detection and response to security threats within its cloud computing environment. The deployment of anomaly analysis and continuous monitoring systems serves as the cornerstone of this policy, enabling the prompt identification and mitigation of suspicious activities. Emphasizing the critical importance of early

threat detection and response, Illumina's policy underscores the pivotal role of advanced detection tools and continuous monitoring systems in bolstering the security posture of its cloud infrastructure. By leveraging these tools, Illumina aims to enhance its capacity to detect and mitigate security incidents effectively, minimizing potential damages. Under this policy framework, Illumina will deploy advanced anomaly analysis tools capable of discerning anomalous behavior within the cloud environment. Concurrently, continuous monitoring systems will be tasked with real-time tracking of system activity, network traffic, and access logs. To validate the efficacy of detection measures, Illumina will conduct regular assessments of anomaly detection tools and monitoring systems. Furthermore, automated alert systems will be implemented to promptly notify security teams of any identified anomalies, facilitating immediate response and investigation protocols to safeguard Illumina's cloud computing environment effectively.

Protect Function:

- Subcategory 1: Stored Data Protection: Implement robust encryption mechanisms to safeguard stored data within Illumina's cloud computing services.
- Subcategory 2: Data in Transit: Utilize encryption and other security measures to ensure secure transmission of data between Illumina's systems and the cloud computing services.

Detect Function:

- Subcategory 1: Anomaly Analysis: Deploy advanced tools capable of detecting unusual or suspicious activities within Illumina's cloud computing system.
- Subcategory 2: Security Continuous Monitoring: Implement continuous monitoring systems to detect and respond to security threats in real-time.

Asset 2: Laboratory Information Management System (LIMS) - System Downtime ([redacted])

Explanation: The Laboratory Information Management System (LIMS) is crucial for managing laboratory operations at Illumina. However, system downtime poses a significant risk, leading to delays in research and testing.

Risk Category/Sub-Category: Information Risk - System Downtime

Rationale: Illumina's LIMS is critical for laboratory operations, and system downtime can lead to significant disruptions. By developing detailed incident response plans and clearly defining roles, Illumina can respond promptly and effectively to downtime incidents, minimizing the impact on research and testing activities. Additionally, having robust recovery procedures and backup systems in place ensures quick restoration of functionality, allowing Illumina to maintain productivity and efficiency during downtime events. This proactive approach helps safeguard Illumina's laboratory operations against disruptions and ensures continuity of critical activities.

Recommended Control:

Respond

Illumina recognizes the pivotal role of timely and effective responses in mitigating the repercussions of system downtime within its Laboratory Information Management System (LIMS). To address this imperative, the company has instituted a comprehensive policy under the response function, focusing on incident response planning and coordination to minimize disruptions to research and testing activities. Under the Incident Response Planning subcategory, Illumina emphasizes the development and regular updating of detailed plans delineating actions to be taken in the event of system downtime. These plans, comprehensive in nature, outline roles, responsibilities, and escalation procedures to ensure a cohesive and efficient response to downtime incidents. Regular reviews and updates of these plans are conducted to accommodate evolving operational requirements and emerging threats, thereby enhancing organizational preparedness and resilience. Furthermore, within the Coordination and Communication subcategory, Illumina aims to establish clear roles and responsibilities for incident response teams and facilitate effective communication during downtime incidents. Specific personnel are designated to coordinate response efforts, disseminate critical information, and liaise with relevant stakeholders, including laboratory staff, IT personnel, and management. Regular communication channels and protocols are established to ensure timely updates and alignment of response efforts across all stakeholders.

Recover

In the event of system downtime within Illumina's Laboratory Information Management System (LIMS), the company employs robust recovery procedures and backup systems to expedite the restoration of functionality and ensure the continuity of critical laboratory operations. This comprehensive approach, encapsulated within the Recover function, revolves around defining and implementing recovery procedures and maintaining backup systems to mitigate the impact of downtime incidents. Under the Recovery Procedures subcategory, Illumina focuses on defining and implementing steps to swiftly recover from system downtime, with a particular emphasis on restoring data and functionality to the LIMS. Detailed recovery procedures outline the sequence of actions, including data restoration processes, system reconfiguration, and verification of system integrity. These procedures undergo periodic testing and refinement to enhance response effectiveness and minimize downtime duration. Furthermore, within the Backup System Setup subcategory, Illumina emphasizes the importance of maintaining backup systems prepared for use to ensure operational continuity in the event of primary system failures. Robust backup solutions are deployed to securely store critical data and system configurations, facilitating rapid recovery and minimal data loss during downtime incidents. Regular backups are conducted according to predefined schedules, with stringent measures in place to safeguard backup integrity and accessibility. Overall, Illumina's comprehensive approach to incident response and recovery within its Laboratory Information Management System (LIMS) underscores the company's unwavering commitment to sustaining operational resilience and ensuring uninterrupted laboratory operations amid downtime incidents.

Respond Function:

- Subcategory 1: Incident Response Planning: Develop and regularly update detailed plans outlining steps to be taken in the event of system downtime.
- Subcategory 2: Coordination and Communication: Establish clear roles and responsibilities for incident response teams and facilitate effective communication during downtime incidents.

Recover Function:

- Subcategory 1: Recovery Procedures: Define and implement steps to recover from system downtime swiftly, focusing on restoring data and functionality to the LIMS.
- Subcategory 2: Backup System Setup: Maintain backup systems ready for use to ensure continuity of operations in case of main system failures.

Asset 1: Phishing attacks against the scientists ([redacted])

Explanation: Phishing email attacks are social engineering attacks that are sent out to steal the personal information from employees. They target individuals' damage and data loss if left attended.

Risk category/sub-category: Data Theft

Rational: Phishing attacks on the scientist and workers at the laboratory can cause security issues, information leaks and damages. The company knows this and realizes that the leading cause of people falling for phishing attacks is human error and a lack of training. To best prevent this from happening, the company needs to invest some of their resources into training their scientists how to identify suspicious emails and report these emails to the proper officials. There needs to be a set of rules and regulations put in place that tells the scientist what to do if they receive a susp absolute certainty. Illumina should also hire an outside company to run a practice phishing attempt on the scientist to see how well they would fare in handling an attack like this.

Recommended Control:

Process of identifying phishing attacks

For a company to mitigate these types of attacks, the company must have a concise set of assets that they know will be targeted in the event of a phishing attack so that they can better protect them. A policy must be put in place for an asset manager to decipher what assets are deemed the most in danger in the event an attack like this were to happen within the company. The asset management team will consider the assets that are most at risk in the event of a phishing attack and will then relay this information over to the risk assessment team, who will then graph out the assets and rank them accordingly from most vulnerable to least vulnerable. In the case of phishing attacks, the most vulnerable assets are usually employee login information, which can be used to gain access into the company's da company so that they can sell the information off to the highest bidder. After measuring the different assets, the risk management team should begin to make policies addressing these risks so that the employees can

steer clear of these attacks. The risk management team is already aware of the fact that even if they try to mitigate the issue of phishing attacks with awareness training for the employees, there are risks which the company is going to have to accept as inevitable when it comes to phishing attacks. The main issue being human error and social engineering attacks that prey on this flaw.

After the teams look at the potential risks and how they can be mitigated, the company will release policies on a company wide scale to enact awareness training to make employees aware that attacks like these are happening. Awareness itrreaianilrogt woofulrdens’oturrceeqsu or money cheap to do. Having company meetings every month to discuss the latest phishing attack trends and having employees be aware of any suspicious emails should be a pretty simple process. Outside of meetings, the same effect can be achieved using flyers and other cheaply produced methods to remind employees that emails sent to them about resetting passwords should only come from the email of the IT department and should have the company's secondary level domain after the at sign within the email. Anything other than that should not be clicked on and should be notified to the IT department and the management department as soon as possible to prevent the spread. While these strategies are not meant to be a definitive solution to prevent phishing attacks, they are a good way at making employees aware of the different types of phishing attacks that could infiltrate their company.

Protections of Assets

For a company to properly protect their assets from phishing attacks, it must have their employees knowledgeable in how these attacks might be implemented against them. With awareness and training, the company can ensure that their employees can be knowledgeable of the types of phishing attacks that they have the potential to encounter. They will be trained on what to do if they were to get a phishing email, which would be to not click on suspicious emails and to not click on any website that the company has not approved of, along with reporting the emails that they receive that seems like a phishing email. There will also be a policy put in place for mandatory meetings every two months with all employees to make sure that their knowledge of phishing attacks is brushed up.

The data security team will have policies put in place for them to monitor the number of phishing attacks that are reported to the IT department, along with any pa important to find a pattern with these attacks so that employees know what to look for to prove their legitimacy. This will prevent a lot of employees from being tricked into thinking that the emails are legitimate and falling for the attack.

Information protection processes and procedures will oversee managing the protection of information systems and assets, by setting restrictions on company devices. There will be a policy put in place to block any site that is not authorized by the company, to prevent the risk of employees accessing a phishing site. They will also oversee programming Illumina's login systems with automatic alerts to the user on the login page every three months, informing them that their password needs to be changed because it is about to expire. A policy will be put in place for the mandatory inclusion of a two-factor authentication sign up for all employees.

This will prevent employees from being tricked easily by fake emails about password resets, thanks to the fact that the reminder will always appear on the actual login screen, never in their emails, as well as prevent unauthorized individuals from gaining access into an employee account if their username and password are compromised.

Maintenance will catalog all the instances of phishing attacks as they come and make a comprehensive data bank of those who have been compromised, along with their credentials, so that their login information can be marked compromised. This will inform the IT department that the user needs changing their passwords and credentials and that their old credentials should be removed from the system.

Identify Function: Understanding the rise of phishing attacks.

- Subcategory 1 ID.AM, ID.RA, and ID.RM: Phishing attacks are the most common type of cyber-attack out there and it is an attack that will inevitably catch an employee due to human error.

Protection Function: Data theft

- Subcategory 1 PR.AT, PR.DS, PR. IP, PR.AC, and PR.MA: Taking the time and resources to train the scientists that work within the lab to know what to look for, when it comes to possible phishing attacks.
- Subcategory 2 PR.AT, PR.DS, PR. IP, PR.AC, and PR.MA: Train the scientist to know how to respond to a phishing attack, in informing them on who they should talk/report to in the event of a phishing attack so no one else is affected by it.

Laboratory equipment ([redacted])

Explanation: Malware infections within the company's proprietary software and hardware can lead to data leaks, data loss, system corruption, hardware damage, etc. This can cost the company millions of dollars in damages, from not only their hardware loss, but also from lawsuits, due to the potential loss of customer data.

Risk category/sub-category: Hardware malfunction and corruption

Rational: Malware within Illumina's lab equipment and soft
corruption of software and possible destruction of systems/machines. It is important that Illumina takes into consideration the importance of having their systems both hardware and software thoroughly scanned for any malware that could cause damage to their data and equipment. Their best response would be to isolate the infected device away from the servers, so that no other devices connected to the servers will be infected and try to resolve/neutralize any malware that is present within those machines. After the malware has been taken care of, recovery efforts for any data that was not affected by the attack should be retrieved and the latest backups should be used so that they are not set back too much. Finally, the company should look back to see what could have been done better to prevent an attack like this from happening again.

Recommended Control:

Active Detection

Malware issues are prevalent within every organization as it threatens to damage hardware and steal the information from software and company data banks. To fight against any form of malware, the company must be able to detect any anomalies and events that might take place within the hardware or software. To achieve this the company can implement a malware/antivirus s level overview of any malware or viruses that might be within the company devices. While these scans aren't designed to prevent malware attacks from happening, devices that might have been overlooked. Having these scans run daily can help Illumina out quite a bit and it's very inexpensive as well. With surface level de to look over malware that can be detected and resolved quickly before it is able to transpire into something bigger and more costly.

Besides basic malware detection, Illumina could also invest in deep scanning their systems to make sure that there is no malware hidden within their systems, staying dormant to prevent detection. These scans tend to be far more thorough and can pick up not only malware, but rootkits, spyware, adware, and viruses can all be detected with relative ease. These scans tend to be more costly and don't need to be done as frequently as surface level scans, as it would just be excessive and a waste of money. Taking this into consideration I would suggest that deep scanning Illumina's network should be done every three months on their networks to ensure that they are not containing any hidden malware that surface scans have failed to pick up on. Deep scanning Illumina's network can help the company det damaging malware before it has the chance to get out of hand and cause serious damage or data loss.

Illumina's continuous monitoring and detection proces transmission to see if all their data is going to the proper location. If the data is interrupted and the full set has not been delivered to their intended destination, Illumina can indicate that the error is not natural and there could be something malicious within the software that is preventing all the data to transfer over. This would then lead to malware scans and anti-malware tactics to see what kind of malware might be on the system. While this method is not a direct detection of malware, it can be used as an indicator that malware might be on the company's network and that action needs to be taken to prevent any more data loss.

Hardware and Software Malware- Responding in the event of an attack (Nicholas)

Before the event of a cyberattack happens on the company, Illumina needs to have a ready to access and planned out response to counter the spread of the malware. This will ensure if a malware outbreak were to occur, there is a precise and easy to follow plan that is already in place to prevent any confusion in the process.

Actual mitigation methods that should be taken into consideration would be for the IT team to isolate any devices that are known to be infected with malware to prevent the spread. There should be a wide and thorough deep scan of all every device that was connected to the network, to see if there were any devices

that were infected but overlooked by mistake. This will prevent any malware from slipping through undetected and continuously infecting systems afterwards.

After the devices have been isolated and the other devices have been deep scanned, an analysis of the malware should be conducted to see what type of malware was on their system. Doing this will give the IT team a better understanding of what the attacker was after, whether it be to steal information from the company to sell off their data, or if it was a company wanting to do damage to their systems by corrupting software and subsequently hardware. It also gives the team an understanding of where the attacker might have originated from, which can also reveal more about their motives.

The next stage would be for the IT team to report their analysis to higher authorities within the company to inform them on the type of attack that has taken place and how much damage the attack did to their hardware and software, along with how much data was lost in the process. Keeping them up to date and telling them the extent of the damages, can help them grasp the full scope of the situation, which can help influence their decision in improving the company's c also be discussed with upper management so that an investigation can be launched.

Finally, improvements on the company's cybersecurity infrastructure should also be discussed and pursued. Illumina would need to investigate and explore all the possible ways in which this malware was able to get into their systems and improve them accordingly. Malware attacks can occur from many different errors and each one of them should be criticized and improved upon to prevent an attack like this from happening again. Banning access from non-company related websites on company de implementing better cyber hygiene training can all be viable options for preventing malware attacks on the company.

Recovering Lost data

In the event of a malware attack on Illumina, it is important to assess the damages after the malware has been eliminated to see how much damage in terms of data loss did the company suffer. This is why it is important that before an attack has even happened, Illumina should have a plan on how the recovery process should be done and take proactive steps to secure the company's data in the most efficient way possible so that the company can get back to track without too much delay. Preparing ahead of time would require Illumina to conduct routine backups of the company's work, DNA samples, patient data, software, etc. These backups should be done preferably every night after the workday has concluded for optimal coverage. However, with the amount of data that Illumina has, it is safe to say that storing all that data would cost a significant amount of money. The more reasonable solution would be to conduct monthly backups to save on money and storage space, while deleting outdated and useless data that just acts as clutter within the storage devices.

After a cohesive plan is made, communications must take place to inform upper management and lower management about the recovery plan so that everything can go a bit smoother. On the other end, after the

event of a malware attack communication efforts must take place to inform patients and law enforcement whose data has been lost without the possibility of being recovered. It is their right to know what happened to their data and how it was affected during the attack. A thorough and easy to digest report must be administered to upper management and shareholders to ensure that recovery efforts are underway and that the company is doing everything in their power to recover as much of their lost data as possible. This will assure investors and shareholders that the company has not taken a significant hit from the attack. This will keep shareholders and investors happy, so they don't get cold feet and pull their money out of the company immediately.

Lastly, improvements should be discussed and made based on the effectiveness of the recovery process. Illumina's recovery team should look back and see what could have been improved during the recovery stage and how more data could/should have been saved in the process to further mitigate the loss. These improvements can be centered around more frequent routine backups, how fast did the recovery team act upon knowing that the attack was resolved, how many people acted etc. Better improvements to the recovery plan can lead to more data being saved and less money the company losses over an attack.

Detection Functions: Malware detection

- Subcategory 1 DE.AE, DE.CM, and DE.DP: Illumina must be capable of scanning their systems on a routine basis to find malware that may be hidden within the company's hardware and software.

Response Function: Response efforts

- Subcategory 1 RS.RP, RS.MI, RS.AN, and RS.IM: The company must find a way to respond properly to the malware breach, to prevent as much data loss as possible.

Recovery Function: Recover data

- Subcategory 1 RC.RP and RC.IM: After the response efforts are done, the company needs to focus on recovering any data that was not impacted by the malware attack and seeing how they can recover any lost data in the process. Also, within the recovery stage it can be used to take a step back and see what could have been done differently.

Asset 1: Point of Sale (POS) System (Emma Humphreys)

Explanation of Asset: Illumina's Point of Sale (POS) system is a facilitating transactions, inventory management, and customer interactions. Conducting a comprehensive risk assessment for the POS system is essential to identify potential vulnerabilities and implement effective controls to safeguard the company's assets and maintain business continuity.

The risk function/category/sub-category

Function: Protect

Subcategory 1: PR.DS (Protect Data Security)

With the flow of credit card details, and PII through their POS system it is vital that Illumina maintains controls in place to keep this information secure. Ensuring that there is end-to-end encryption and the software used to run the POS is regularly updated and patched will prevent the leakage of data while it is in transit.

Subcategory 2: PR.IP (Information Protection Processes and Procedures)

To secure credit card transactions and sensitive data collected during online sales, Illumina should adopt robust encryption measures, strictly limiting access to authorized personnel. Regular monitoring and audits are essential to detect and prevent unauthorized access attempts.
Clear guidelines should govern data handling and disposal, with staff training programs ensuring compliance. Automated protocols for deleting records post-transaction will help manage personal information effectively. These measures mitigate risks, safeguard customer data, and maintain regulatory compliance.

Recommended Controls:

To address the subcategory of Protect Data Security (PR.DS) within Illumina's Point of Sale (POS) system, it's crucial to establish policies and procedures that mitigate risks associated with handling sensitive data such as credit card details and personally identifiable information (PII). This involves implementing a policy specifically focused on Data Security Protection, aimed at safeguarding sensitive data processed through the POS system by enforcing robust security measures. Policies directly addressing PR.DS should focus on protecting data integrity and confidentiality within the POS system through measures like end-to-end encryption and regular software updates. One procedure to support these policies would be to enforce regular software updates and patch management, which outlines steps to ensure that the software running the POS system. This would also include regular updates and patches to address vulnerabilities and mitigate the risk of data breaches. To implement this, a designated IT team could be assigned responsibility for monitoring updates and patches, with a schedule established for regular maintenance to minimize disruption. A validation control, vulnerability scanning and penetration testing, involves conducting regular assessments on the POS system to identify and address potential security weaknesses. This could be achieved through quarterly vulnerability scans and annual penetration tests, utilizing both automated scanning tools and external security experts. Additionally, an Incident Response Plan can serve as a validation control, outlining steps to be taken in the event of a data breach or security incident involving the POS system. Regular tabletop exercises can be conducted to test the effectiveness of the plan and ensure that all relevant personnel are familiar with their roles and responsibilities. By implementing these policies, procedures, and controls, Illumina can enhance the security posture of its POS system, safeguard sensitive data, and maintain business continuity.

Information Protection Process & Procedures

In Illumina's business operations, effective management of sensitive data collected during online sales transactions through the Point of Sale (POS) system is paramount. The subcategory of PR.IP (Information Protection Processes and Procedures) is particularly critical in this regard, given the nature of transactions involving credit card information and personal or business addresses and names. To mitigate risks associated with unauthorized access or misuse of this data, robust policies and procedures must be in place.
A recommended control is the adoption of encryption for all credit card transactions, both during data transmission and while stored. Encryption renders data unreadable to unauthorized individuals, safeguarding it from interception or exploitation. This aligns with the NIST framework's principle of safeguarding data at rest and in transit.

Strict access controls should also be enforced to limit access to credit card data solely to authorized personnel with legitimate business needs. This entails implementing user authentication mechanisms, such as strong passwords or biometric authentication, and role-based access controls. Regular monitoring of user activities and access logs can help detect and prevent unauthorized access attempts.

Illumina should establish clear guidelines and protocols governing the handling and disposal of sensitive data collected through the POS system. Training programs should be provided to employees to ensure they understand their responsibilities regarding data protection. Regular audits and assessments should be conducted to evaluate the effectiveness of existing controls.

As a validation measure, Illumina can implement regular review and analysis of access logs and audit trails to verify compliance with established policies and procedures. This involves monitoring access attempts to credit card data, detecting any anomalies or unauthorized activities, and taking appropriate remedial actions. Periodic penetration testing and vulnerability assessments can help identify potential weaknesses in the POS system's security posture.

In summary, by implementing robust policies and procedures for information protection within its POS system, Illumina can effectively mitigate risks associated with the handling of sensitive data, ensuring the security and privacy of customer information. Regular monitoring, assessment, and validation of these controls are essential to maintain compliance with regulatory requirements and industry best practices, thereby safeguarding the company's assets and maintaining business continuity.

Asset 2: Illumina Proactive Instrument Performance Services (Emma Humphreys)

Explanation of Asset:

Illumina Proactive Instrument Performance Services are designed to optimize the performance of Illumina sequencing instruments and ensure reliable and accurate results. However, like any service, there are potential risks associated with its implementation. A thorough risk assessment is crucial to identify, evaluate, and mitigate potential issues, thereby ensuring the effectiveness and safety of the service.

The risk function/category/sub-category

Function: Identity & Protect

Subcategory 1: ID.BE-5 (Identity Business Environment-5)

The subcategory ID.BE-5, falling under the function Identity & Protect, underscores the importance of employing multi-factor authentication (MFA) mechanisms to safeguard identities accessing organizational resources. Illumina's Proactive Instrument Performance Services seamlessly align with this objective by implementing stringent identity verification processes for users accessing instrument performance data and diagnostics. By mandating multi-factor authentication for users accessing such data through Illumina Proactive Instrument Performance Services, Illumina ensures the integrity of its systems, thereby enhancing the protection of sensitive genetic data against unauthorized access or tampering. This alignment with NIST guidelines underscores Illumina's steadfast commitment to maintaining the highest standards of security and confidentiality in its genomic services.

Subcategory 2: Protect –PR.MA-1 (Protect Maintenance-1)

This subcategory emphasizes the necessity of protecting systems from unauthorized access and ensuring the integrity of maintenance activities. With Illumina Proactive Instrument Performance Services, regular maintenance and performance monitoring are essential to ensure uninterrupted operation and accurate results. By implementing robust access controls and rigorous validation processes, Illumina safeguards its instruments against unauthorized modifications or disruptions, aligning with PR.MA-1's objectives and reinforcing confidence in data integrity and instrument reliability.

Recommended Control

IIllumina should meticulously implement robust recommendation controls to align with NIST Subcategory 1: ID.BE-5 (Identity Business Environment-5) and Subcategory 2: Protect –PR.MA-1 (Protect Maintenance-1) guidelines. Upholding ID.BE-5 involves securing its identity business environment through multi-factor authentication protocols, stringent access controls, and regular identity verification processes. This ensures that only authorized personnel can access sensitive data and systems, effectively minimizing identity-related breaches. Meanwhile, adhering to PR.MA-1 necessitates proactive measures to safeguard infrastructure and assets through continuous monitoring, patch management, and regular system updates.

To mitigate associated risks and ensure compliance with standards like NIST guidelines, Illumina adopts comprehensive policies and procedures. For instance, it mandates multi-factor authentication (MFA) for all users accessing instrument performance data and diagnostics via Proactive Instrument Performance Services. Users are required to provide credentials and set up MFA methods such as biometric verification, SMS codes, or authenticator apps upon registration. When accessing data or diagnostics, users undergo authentication through at least two factors. Regular reviews and updates of MFA methods and access privileges maintain alignment with security standards and organizational needs. Through training sessions, users are educated on the importance and usage of MFA. Periodic audits validate MFA compliance by

scrutinizing access logs and authentication records, while penetration tests simulate potential attacks to assess MFA effectiveness. User feedback helps identify usability issues, and incident response investigations evaluate MFA's role in preventing unauthorized access.

Additionally, to mitigate risks associated with Illu
with PR.MA-1, robust policies and procedures are imperative. This includes enforcing stringent access controls and validation measures to protect systems and uphold maintenance activity reliability. Illumina enforces strict access controls, incorporating MFA protocols and an authorization matrix to define roles and permissions. A robust change management process oversees maintenance activities, complemented by comprehensive audit trails and regular security best practice training. Regular audits and assessments validate the effectiveness of implemented policies and procedures, examining access controls and validation procedures. Furthermore, penetration testing evaluates the system's resilience against cyber-attacks, while incident response drills assess the organization's response capabilities. A feedback mechanism enables employees to report security concerns, contributing to a proactive approach in safeguarding operations and customer data. Through these measures, Illumina effectively mitigates risks associated with unauthorized access, ensuring the integrity of maintenance activities, and safeguarding its operations and customer data.

Conclusion

Illumina's is one of the leading genetic companies in the world and their innovations and contributions to the field has no signs of slowing down. However, it is important that the company knows their weaknesses and compensate for them appropriately, as the repercussions of their lack of actions could endanger the information and lives of millions of patents, while also putting the company into serious legal risk. With the amount of bio-genetic technology that the company has on offer, it is of the utmost importance that the company focuses on protecting its database and network from any outside attack that may befall them.