Risk Assessment Report

for

Health & Wellness Partners, LLC (HWP) -

A Medical and Scientific Communications Agency

Prepared by: Lauren Patasnik

Report Date: December 13, 2024

INST464-0101

Table of Contents

About this Document

Project Description

This report reflects a cybersecurity risk assessment of Health & Wellness Partners, LLC (HWP), a provider of medical communications solutions to global life sciences companies. They are headquartered in Upper Saddle River, NJ and work both hybrid and virtually to serve their clients across the U.S. HWP's mission is to improve the lives of their clients' patients by providing educational materials and unique digital solutions.

Key Terms

No special terms have been used in this cybersecurity risk assessment.

Limitations

This cybersecurity risk assessment is based on an external analysis of Health & Wellness Partners, LLC (HWP) through their website and products. No contact was made with employees or their clients which limits understanding of business processes and specific vulnerabilities. Multiple quantities were inferred or taken from case studies and articles to support the recommendations made in this report.

Analytical Confidence

I assessed the analytical confidence of this assessment as Medium.

I've discovered their most prominent assets along with vulnerabilities they are likely to face. These are deeply analyzed in the risk scenarios described later on along with associated quantified loss. I've assessed the confidence in probability of loss and magnitude of loss as medium because inferences were made using similar companies. There is medium confidence in potential losses because quantities of loss were taken from previous case studies in the medical field. Overall, this results in an analytical confidence level of medium for this risk assessment for HWP.

Executive Summary

This is an analysis of Health & Wellness Partners, LLC (HWP) along with recommendations for cybersecurity improvements and business operations.

Based on my analysis, I've come up with a list of recommendations for HWP to limit any potential loss they may experience. I have one major cybersecurity recommendation, four cybersecurity actions to take, and two suggestions for better practices. After undergoing these changes, the total cost will be around $70K per year which will reduce the risk of a major loss scenario occurring to a 3% risk per year of a $15K loss. This is compared to the current loss scenario of around $1M per year and a 50% probability of a $200K loss.

The major cybersecurity recommendation is for HWP to implement Multi-Factor Authentication for all user accounts. This will minimize the compromise of accounts by requiring an additional form of identification by users. If hackers were to obtain a password list, it would be useless because they would need more than just a password to gain access into user accounts.

Next, there are four cybersecurity actions to implement that will also contribute to less risk for HWP. The first step to take is to implement a better Access Control System to ensure patient data is only viewed by authorized personnel and remains compliant with regulations. Next, implementing behavior analytics to be able to monitor unusual patterns or activity if users are signing on through different devices or locations. Next, having stronger encryption of solutions and patient data in the instance it ends up in the wrong hands. Lastly, regularly conducting penetration testing to identify vulnerabilities in your system which could lead to breaches and unauthorized access. All four of these actions will reduce the risk of loss of patient data, user account info, and HWPs Proprietary Digital Solutions.

Lastly, I suggest HWP to highly focus on their employees and interactions with cybersecurity practices. Human error can have lasting impacts on a company and employee training is something that can be focused on. In addition, having an official Incident Response Plan will allow everyone to be prepared in the event of a real-life cybersecurity attack. These practices will lead HWP to success and allow them to be better prepared in the event of a cybersecurity threat.

Company Overview

This cybersecurity assessment is on a medical communications company, Health & Wellness Partners, LLC (HWP). They began and are currently located in Upper Saddle River, NJ and work both hybrid and virtually to serve their clients across the U.S. HWP's mission is to improve the lives of their clients' patients by providing educational materials and various digital solutions. Their clients include but are not limited to pharmaceutical companies and health practitioners who can then better provide for their patients.

HWP was founded and started in 2005 by three women, Jani Hegarty, Audrey Pezzuti, Bonnie Welsch. Their headquarters, known as HWP East, are located in Upper Saddle River, NJ. Later on they built a second office, known as HWP West, located in San Diego, CA. They are a privately held company who doesn't raise funding so the founders can maintain complete control of the company and their mission for the benefit of their clients. They fall under the life sciences industry who specializes in four services which include medical marketing, medical affairs, speaker bureau, and congress management. HWP currently has around 240-265 employees who have the ability to work remotely and still provide for their clients. HWP provides assistance in a variety of ways including expert opinions, tailored technology, and engaging education sessions, making sure they continue to carry out their mission of improving the lives of patients and putting people first.

HWPs estimated annual revenue is around $27 million (reported in 2024) with profit margin unknown to the public. We can assume that business has been successful for them due to investments from NMS Capital, their partner Hybrid Healthcare Communications LLC, and their growing list of clients such as Pfizer, Johnson & Johnson, Acadia, Genentech, and more.

They host their main website on one main server which provides public information on who they are as a company, their services, mission, business operations, and further resources. They have an internal platform which facilitates communication for customers and clients. This requires login credentials which will then allow access to more resources, solutions, and engagement. Depending on their credentials, they will have authorization to different kinds of information, which can include sensitive data.

HWP has a range of leadership roles including Chief Executive Officer, Director of Accounting Services, Senior VP of IT, Senior VP of Scientific and Medical Services, and Managing Director of Speaker Bureau. All roles have a range of responsibilities but deal with organizational strategies, client relationships, managing IT, and content development. They all contribute to maintaining relationships with their clients and providing solutions for their needs. They will generally have access to their clients' patient medical records and unique information pertaining to their digital solutions they've developed. They also have access to educational materials which are personalized for their clients and patients.

HWP is mostly known for their Proprietary Digital Solutions which are supported by data and designed to drive decision-making for their clients. These solutions give them a competitive advantage because of its personalization to clients needs and requirements. HWP continues to deliver innovative technology while supporting their mission of improving the lives of their clients' patients.

HWP uses Microsoft 365 and its product Office365 as their emailing system. This service allows them to carry out everyday business operations such as communicating with clients, hosting virtual appointments, delivering solutions, and more. HWP also has strong cybersecurity practices in place to maintain their system and confidentiality. They have implemented Cloudflare and Proofpoint to mitigate risk and protect sensitive data, both which are very important for the medical industry. Proofpoint offers benefits such as email security, encryption and threat management. This contributes to HWPs knowledge of cybersecurity and their interest in protecting their whole network from any cybersecurity threats.

Qualitative Risk Analysis

After assessing HWP, there are three main areas of risk to take note on:

- Unauthorized Disclosure of Patient Information through healthcare practitioners
- Loss of User Account Information and Patient Data by cyber groups or individual hackers.
- Breach of Proprietary Digital Solutions via cyber group or attack

Risk related to patient data could be severe and result in a large magnitude of loss along with medium probability of occurrence. Risk related to user account information and Proprietary Digital Solutions are less and would result in a medium magnitude of loss and probability of occurrence.

Assets

HWPs physical assets include the information they hold at their office locations in Upper Saddle River, NJ and San Diego, CA. Here they conduct their operations and further advance their Proprietary Technology.

HWP information assets include sensitive patient records and data, scientific research and data, emails, user credentials, and client information. All information is stored remotely on the Office365 platform, which is secured through Proofpoint. HWP produces their Proprietary Digital Solutions which are technology-driven and support their medical marketing, medical affairs, speaker bureau, and congress management services. This allows them to deliver innovative, educational products to their clients to achieve their goals.

Threat Vectors

HWP is likely to experience a breach of confidentiality or integrity of their assets including patient information, user account information, or their Proprietary Digital Solutions. They can be targeted for patient records which can then be exploited or used as a motive for payment. These can be obtained through phishing attacks against employees, ransomware, or finding any existing vulnerability in their server.

To manage communication and solutions for clients and other stakeholders, HWP offers a third-party service known as hwpconnect. This platform is a place for them to access resources and materials specifically meant for them and can only be accessed using their credentials. This makes it more difficult for hackers to access the server from the outside, as well as easily access any credentials.

Threat Actors

HWP is likely to be targeted by a cybercriminal group, script kiddie, or an individual hacker. It is possible for them to launch a phishing attack against an employee or find a vulnerability within

their system. Their motivation may be to obtain personal identifiable information or payment from the company. Hacktivists are less likely to target HWP because they are a small company who are transparent about the work they are doing.

Losses

HWP losses are separated according to each risk scenario described below.

The first category of loss is linked to the **unauthorized disclosure of patient information** through healthcare practitioners. There is no direct loss because business operations will keep running and this loss will not affect day-to-day operations. But, HWP is required to notify all patients whose information was impacted which requires funds to send a notice to each one. This can cost around $100K-$200K. In comparison, secondary losses are much larger due to lawsuits and settlements that follow this incident. Multiple patients whose information was unknowingly breached could sue leading to various lawsuits. HWP would require legal representation and lead to costs for a settlement. This could average out to about a loss of $2M to $4M, depending on the size of the breach. Also, HWP could find themselves facing regulatory and compliance fines which average around $25K-$50K. Lastly, it's not unlikely that they could face reputational damage where clients will seek a different company to satisfy their needs. If 20% of clients were to leave, this could result in a loss of around $3M.

The second category of loss relates to the **loss of user account information and patient data** by cyber groups or individual hackers. There would be no direct losses but this incident would require notices to those affected and investigations. This contributes to secondary loss, including $2M in legal fees and settlement, $10K-$25K in investigation, and $25K in compliance fines.

The third category of loss relates to the **loss of HWPs Proprietary Digital Solutions**. Primary loss can include immediate response cost to get back their stolen solutions. This can range around 120K to 1M which includes hiring outside help and paying employees to resolve the issue. Next, secondary losses include around $2M of reputational damage and the cost to rebuild their system which could range around another $2M.

Scenarios

This chart transfers the major losses described above into risk scenarios

Asset	Threat Methods	Threat Actors	Loss Types	Scale of Each Loss Type
Patient Information	Phishing Ransomware Data Breach DDoS Attack	Cybercrime Groups Script Kiddies Individual	Loss of PII Alert Patients Lawsuits	Direct Loss: $0 Secondary Loss: Notices:

	Insider Threat		Reputational Damage (20% customers leave) Regulatory/Compliance Fines	~$380/medical record * 500 patients =~$200K Legal fees & settlement: ~$4M Client Loss: ~$3M Fines: ~$25K
User Account Info	Direct Hack Phishing	Cyber Group Script Kiddies Individual	Loss of PII Alert Patients Investigation Lawsuits Regulatory/Compliance Fines	Direct Loss: $0 Secondary Loss: Notices: ~$380/medical record * 500 patients =~$200K Investigation fees: ~$25K Legal fees & settlement: ~$2M Fines: ~$25K
Proprietary Digital Solutions	DDoS Attack Ransomware Supply Chain Attack Data Breach	Cybercrime Groups Hacktivists Script Kiddies Individual	Loss of Solutions/Immediate Response Cost Reputational Damage (customers leaving - drop in revenue) Cost to restore	Direct Loss: $120K Secondary Loss: Client Loss: 10% customers leave ~$2M Rebuild: $2M

Scenario 1 - Loss of Patient Information: The risk of loss of patient information through hacking is fixed at 7% per year. This risk is driven by the want for patient information to exploit. The estimated direct losses are estimated at $0K while secondary losses are estimated from $2M to $4M due to alerting affected patients, lawsuits, reputational damage, and regulatory fines. The main risk with communicating with other healthcare professionals is violating compliance relating to patient privacy. Through communicating with other practitioners, this opens up opportunities for hackers to gain access to unauthorized information. This kind of loss can be prevented in the future with better administrative controls and cybersecurity measures which will be discussed in the recommendation section.

Scenario 2 - Loss of User Account Info & Patient Data: The risk of loss of patient accounts and passwords (therefore patient data) is assessed at 4% per year. This risk can be driven by gaining access to HWPs restricted resources and knowledge not open to the public. Depending on the user and their authorization, the cyber group or entry-level hacker can gain access to different kinds of sensitive information. While there are no estimated direct losses, secondary losses can be estimated from $1M to $2M. This is due to alerting people impacted, investigation fees, lawsuits, and compliance fines. Depending on the attack and size of those impacted, secondary loss ranges in price. This loss can be prevented with the implementation of Multi-Factor Authentication which will be expanded on in the recommendations section.

Scenario 3 - Loss of Proprietary Digital Solutions: The risk of loss of their Proprietary Digital Solutions is assessed at 2% per year. Direct losses can be estimated around $120K to $1M in efforts to immediately repair their systems. On the other hand, secondary losses range from $2M to $4M due to reputational damage and the cost to rebuild the system. It's important to quickly rebuild in order to preserve their solutions and competitive advantage against other companies. This loss can be prevented with stronger encryption and periodic penetration testing which will be explained further in the recommendations section.

This Heat Map displays the following scenarios based on likelihood and consequence:

Certain >90%				
Very Likely 65%-90%				
Likely 35%-90%				
Unlikely 10%-35%		**Scenario: Loss of User Account Info**		**Scenario: Loss of Patient Data**
Possible <10%		**Scenario: Loss of Proprietary Solutions**		
Likelihood ↑ Consequence →	**Insignificant**	**Minor**	**Moderate**	**Major**

Quantitative Risk Analysis

Pre-Mitigation Loss Analysis - Scenario 1 - Loss of Patient Information

As described above in the Qualitative Analysis Section, Scenario 1 covers loss of patient information due to a breach by a cyber group or individual. This was made possible because of the disclosure of information between HWP and healthcare practitioners, allowing for easier access to the patient information.

Baseline probability: 15%, Minimum value: 10%, Most likely: 15%, Maximum value: 20% - these values are used as a guide for vulnerability; frequency of occurrence ranges from 3-6.

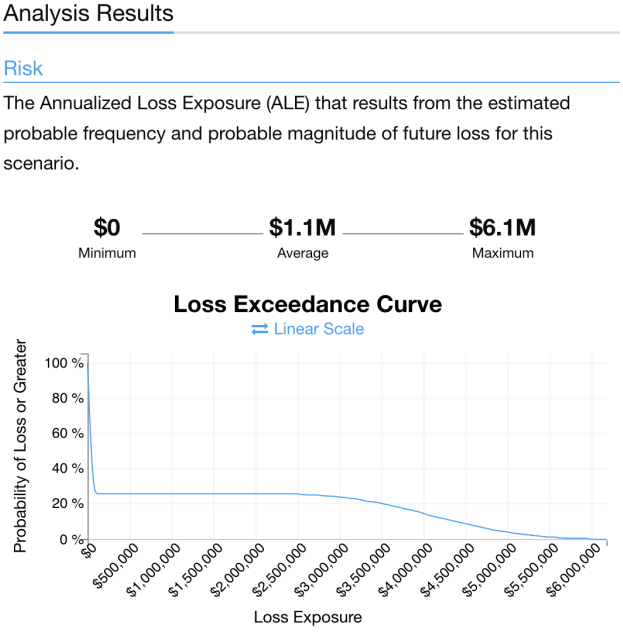
Minimum value is: 3, most likely value: 4: maximum value: 6.

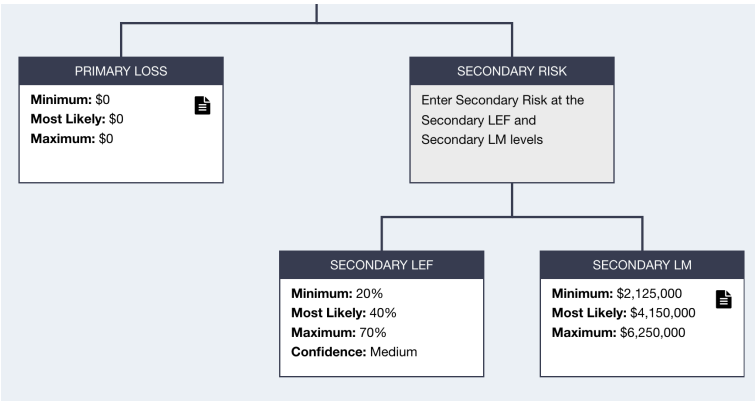
Direct losses: $0.

Secondary losses: $100-200K for alerting impacted patients; $2M-$4M for legal representation and settlements; $25K-$50K for compliance regulations; $0M-$2M in reputational damage.

Overall probabilities: Minimum value: 20%, most likely value: 40%, maximum value: 70%.

In all, these numbers produce the Loss Exceedance Curve below using the Fair-U App.

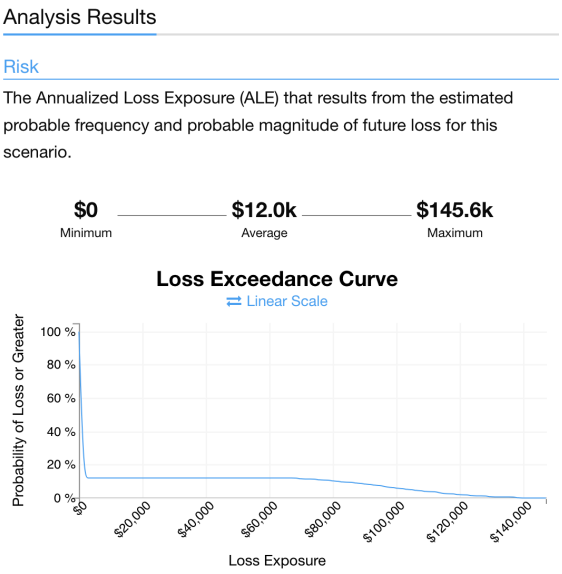




Post-Mitigation Loss Analysis - Scenario 1 - Loss of Patient Information

As briefly explained earlier, the risks associated with patient information include hackers exploiting it for their own gain or selling it to others on the dark web to make money. By implementing better access controls where only authorized users have access to certain resources, this can prevent breaches of information and loss. In addition, implementing employee security training to update them on the best security practices along with continuous monitoring of the network and conducting audits often are both efficient ways of lessening this risk scenario. This being said, the new baseline probability will drop to 7% per year. All other values stay the same.

After taking these steps, which cost a total of $3K, the annual average risk of loss will change from $1.1M to $12K and the maximum loss drops from $6.1M to $145K. The minimum loss remains unchanged at $0. The post-mitigation of implementing training, continuous monitoring, and conducting audits often results in a less risky curve which should be an acceptable amount of risk for the company.

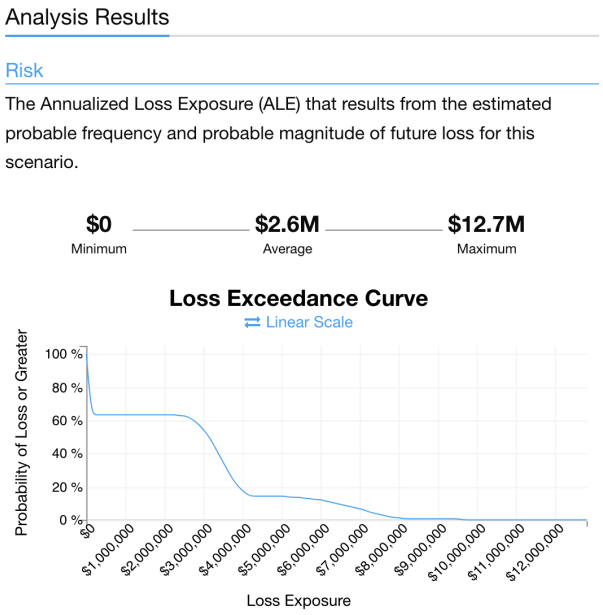


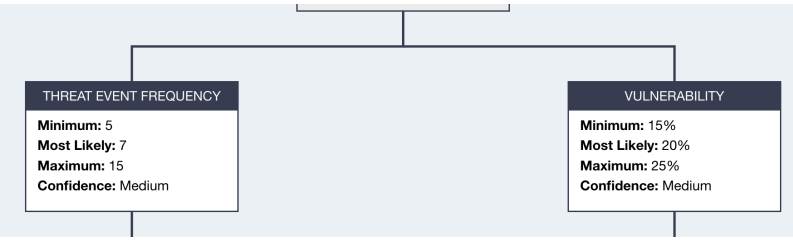
Pre-Mitigation Loss Analysis - Scenario 2 - Loss of User Account Info & Patient Data

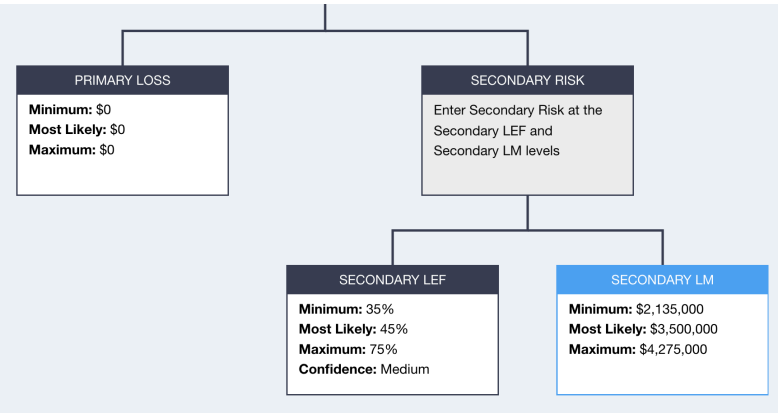
As described above in the Qualitative Analysis Section, Scenario 2 covers loss of user account information and patient data due to a breach by a cyber group or individual. This was made possible because of the password list getting leaked to hackers and no security flags were raised. Baseline probability: 20%, Minimum value: 15%, Most likely: 20%, Maximum value: 25% - these values are used as a guide for vulnerability; frequency of occurrence ranges from 5-15. Minimum value is: 5, most likely value: 7: maximum value: 15.

Direct losses: $0.

Secondary losses: $100-200K for alerting impacted patients; $10K-$25K for a digital forensics investigation, $2M-$4M for legal representation and settlements; $25K-$50K for compliance regulations Overall probabilities: Minimum value: 35%, most likely value: 45%, maximum value: 75%.
In all, these numbers produce the Loss Exceedance Curve below using the Fair-U App.







Post-Mitigation Loss Analysis - Scenario 2 - Loss of User Account Info & Patient Data
As briefly explained earlier, the risks associated with user account information and patient data include hackers gaining access to HWPs restricted resources and any knowledge not open to the public. Depending on the user and their authorization, the hacker can gain access to different kinds of sensitive information that could be detrimental if it were to be released to a bigger audience. By implementing Multi-Factor Authentication, this adds an additional layer of security, requiring another form of authentication. This way, if a hacker were to gain access to a password list, it would be useless without providing another form of unique identification. Also, implementing behavior analytics can better identify potential security threats through employee logins. This being said, the new baseline probability will drop to 8% per year. All other values stay the same.
After taking these steps, which cost a total of $51K, the annual average risk of loss will change from $2.6M to $4.3K and the maximum loss drops from $12.7M to $47.5K. The minimum loss

remains unchanged at $0. The post-mitigation of implementing MFA and behavior analytics results in a less risky curve which should be an acceptable amount of risk for the company.

Analysis Results

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

Pre-Mitigation Loss Analysis - Scenario 3 - Loss of Proprietary Digital Solutions

As described above in the Qualitative Analysis Section, Scenario 3 covers loss of HWPs Proprietary Digital Solutions due to a breach by an entry-level hacker or group. This was made possible because of a possible vulnerability exploited in their system. Therefore, the hacker found their way into their server and obtained insider knowledge on their digital solutions and internal work.

Baseline probability: 9%, Minimum value: 7%, Most likely: 9%, Maximum value: 15% - these values are used as a guide for vulnerability; frequency of occurrence ranges from 5-15.

Minimum value is: 5, most likely value: 7: maximum value: 15.

Direct losses: $120K-$1M for repair costs of the system; Minimum value: $120K, most likely value: $450K, maximum value: $1M.

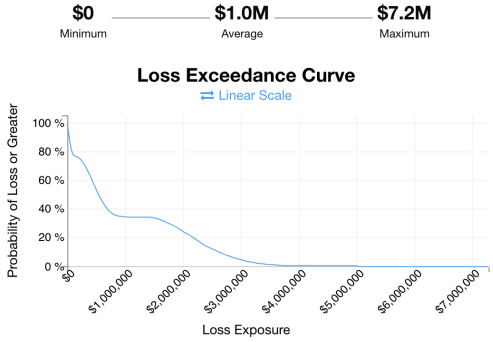
Secondary losses: $0-2M for reputational damage; $1M-$2M to rebuild the system. Overall probabilities: Minimum value: 30%, most likely value: 40%, maximum value: 70%.

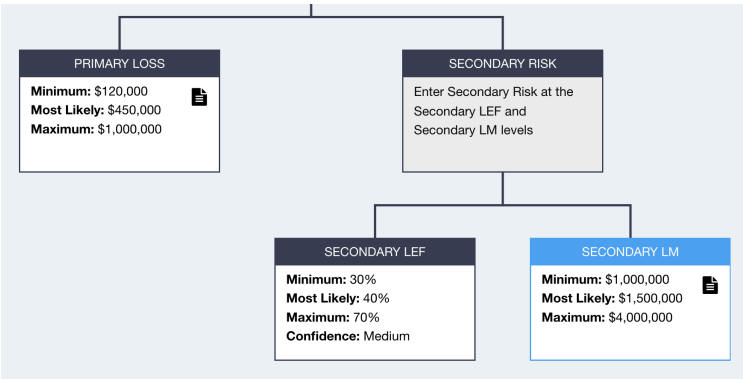
In all, these numbers produce the Loss Exceedance Curve below using the Fair-U App.

Analysis Results

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

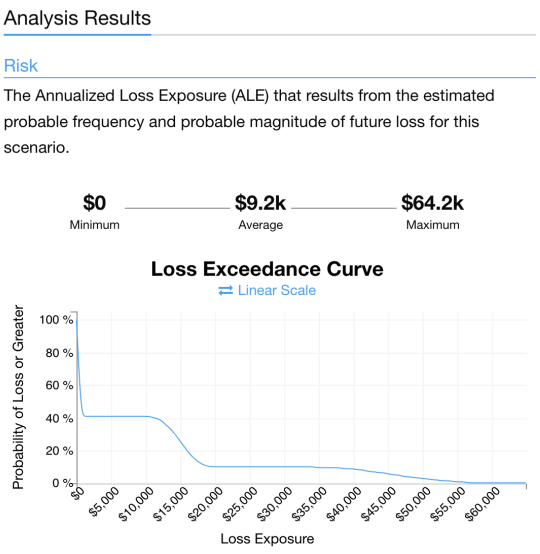




Post-Mitigation Loss Analysis - Scenario 3 - Loss of Proprietary Digital Solutions

As explained earlier, the risks associated with HWPs Proprietary Digital Solutions include hackers gaining access to their private solutions and unique research only meant for themselves and specific clients. These solutions are tailored to their clients needs, giving them a competitive advantage over other companies. If they were to be released without authorization, this would take away their advantage. By implementing stronger encryption, better incident response, and periodic penetration testing, this will lessen the risk of their digital solutions being exposed to unauthorized users. This being said, the new baseline probability will drop to 5% per year. All other values stay the same.

After taking these steps, which cost a total of $15K, the annual average risk of loss will change from $1M to $9.2K and the maximum loss drops from $7.2M to $64.2K. The minimum loss remains unchanged at $0. The post-mitigation of implementing better encryption, incident response, and periodic penetration testing results in a less risky curve which should be an acceptable amount of risk for the company.



Recommendations

Based on my analysis, I've come up with a list of recommendations for Health & Wellness Partners LLC to limit any potential loss they may experience. I have one major cybersecurity recommendation, four cybersecurity actions to take, and two suggestions for better practices. After undergoing these changes, the total cost will be around $70K per year which will reduce the risk of a major loss scenario occurring to a 3% risk per year of a $15K loss. This is compared to the current loss scenario of around $1M per year and a 50% probability of a $200K loss.

The major cybersecurity recommendation is for HWP to implement Multi-Factor Authentication for all user accounts. This will minimize the compromise of accounts by requiring an additional form of identification by users. If hackers were to obtain a password list, it would be useless because they would need more than just a password to gain access into user accounts. Currently, loss of user account info faces a risk of 7% per year costing around $570K. The cost to apply Multi-Factor Authentication is based on the size of the organization and should cost around 1K or more which is more than worth it in the long run.

Four cybersecurity actions to implement will also contribute to less risk for HWP and cost around 3K, 50K, 5K, and 10K each which will be $68K total per year. The first step to take is to implement a better Access Control System to ensure patient data is only viewed by authorized personnel and remains compliant with regulations. Next, implementing behavior analytics to be able to monitor unusual patterns or activity if users are signing on through different devices or locations. Next, having stronger encryption of solutions and patient data in the instance it ends up in the wrong hands. Lastly, regularly conducting penetration testing to identify vulnerabilities in your system which could lead to breaches and unauthorized access. All four of these actions will reduce the risks of loss of patient data, user account info, and HWPs Proprietary Digital. They will also contribute to less primary and secondary losses due to less regulatory compliance violations and lawsuits/settlements. After spending around $68K on these cybersecurity actions, your average loss will change from $1.1M a year to $15K a year.

Lastly, I suggest HWP to highly focus on their employees and their interactions with cybersecurity practices. Human error can have lasting impacts on a company and employee training can be one of the most important things to improve in. Guiding training sessions for employees will reduce human error and teach ways in how to avoid phishing attacks and best utilize technology. This will be most efficient for the company and allow the employee to excel in their technological skills. In addition, having an official Incident Response Plan will allow everyone to be prepared in the event of a real-life cybersecurity attack. It's important to often practice this plan and conduct drills in order to know how to respond and recover appropriately most efficiently. These practices will lead HWP to success and allow them to be better prepared when faced against cybersecurity threats.

Appendix 1: References

https://www.forbes.com/sites/maneetahuja/2020/05/12/forbes-small-giants-25-companies-that-believe-smaller-is-better/

https://www.forbes.com/sites/monicamelton/2020/05/12/wellness-in-a-pandemic-behind-the-women-led-medical-consultancy-navigating-growth/

https://nms-capital.com/news/nms-capital-announces-partnership-with-and-investment-in-health-wellness-partners/

https://www.healthcurity.com/how-much-does-a-breached-healthcare-record-cost/#:~:text=A%20cyberattack%20affecting%20any%20type,hospitals%20to%20recover%20from%20events.

https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement#:~:text=HIPAA%20violation:%20Unknowing,annual%20maximum%20of%20$1.5%20million

https://purplesec.us/learn/data-breach-cost-for-small-businesses/

https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf

https://www.linkedin.com/pulse/strengthening-cybersecurity-healthcare-lessons-from-recent-vonxe/