Risk Assessment Report

for
Plaid

Name: Wonwoo Choi
Date: December 13th, 2024
INST464-102

Table of Contents

ABOUT THIS DOCUMENT **3**

PROJECT DESCRIPTION 3
KEY TERMS 3
LIMITATIONS 3
ANALYTICAL CONFIDENCE 3

EXECUTIVE SUMMARY **4**

COMPANY OVERVIEW **5**

QUALITATIVE RISK ANALYSIS **7**

QUANTITATIVE RISK ANALYSIS **13**

RECOMMENDATIONS **23**

APPENDIX A **25**

REFERENCES **26**

About This Document

Project Description

This document is a security risk assessment report for Plaid, a fintech company founded in San Francisco, and has branches across the world. Plaid provides several banking applications and online merchants services for their customers to securely transfer money and provides its own customers to manage their financials in an encrypted platform.

Key Terms

Salting data: refers to a technique in data processing, where random string (salt) is added to a piece of data before hashing it. It significantly improves security by making it harder to crack the data using precomputed tables.

Limitations

This cybersecurity analysis is based upon external online assessments of the Plaid platform and discusses with key Plaid leaders such as CEO, IT manager, and security team. Direct observation of the company's physical configuration, and day-to-day behaviors of employees was not made. In addition, due to the fact that Plaid is a private company, only estimation of their revenue was used. Therefore, this assessment may be missing vulnerabilities and risks related to physical configuration, and user behavior that is not in compliance with best security practices, and may lack providing evidence in recommendations.

Analytical Confidence

I assess the analytical confidence of this project as: Medium

Plaid has well defined assets and clear documentations of their cybersecurity practices. The vulnerabilities are not well defined and known, but data is rich enough to create a clear analysis of risk management. Confidence in the probability of loss is medium. As stated in the limitation, the company is a private company which makes it hard to access financial information, making it a estimation of loss, instead of an exact number figure, making it medium-low confidence in analyzing amounts of potential losses.

Executive Summary

This security risk assessment evaluates Plaid, a fintech company providing encrypted financial transaction services, focusing on risks to its cloud servers, user data, and intellectual property. The analysis highlights three primary risk scenarios and offers actionable recommendations for mitigation.

Key Risks:

1. **Loss of Cloud Server**: Potential disruptions due to DDoS attacks, ransomware, insider threats, or misconfiguration. The annual probability is estimated at 15%, with losses ranging from $300K to $22.5M, including legal and reputational damages.
2. **Loss of User Data**: Compromises in user credentials or transaction records due to hacking, phishing, or insider espionage. Estimated annual loss could reach up to $65M, with significant impacts on regulatory compliance and customer trust.
3. **Loss of Intellectual Property**: Theft of encryption methods or API details through hacking or insider action. While direct losses are negligible, reputational damage could lead to future revenue losses of $5M–$20M.

Recommendations:

1. **Critical Priority**: Invest $1M to enhance user data security through regular vulnerability assessments, employee training, and stronger database protections. This could reduce user data breach risks to below 1%.
2. **High Priority Actions**:
    - Allocate $300K to secure cloud servers, including redundancy measures, monitoring, and advanced threat detection.
    - Address known vulnerabilities and ensure prompt patching to prevent data breaches.
3. **Best Practices**:
    - Conduct phishing simulations and cyberattack drills to improve employee preparedness.
    - Establish clear incident response protocols to minimize operational downtime.

Implementing these measures, with a total investment of $1.5M, could reduce Plaid's risk exposure from $4.5M annual average losses to under $200K, significantly improving resilience against cyber threats.

Company Overview

Plaid is a fintech company that facilitates communication between financial service apps and users' bank and credit card providers. It allows users to do transactions, keeping customer information encrypted and private. It connects bank to apps powering thousands of apps that people rely on to manage financial transactions: Venmo, Betterment, Chime, Dave, and more. They encrypt the data that the user has chosen to share and securely share it with the app the user wants to use. The user controls whom the user's data is shared with, for what purpose, and how long. The data includes account and routing number, account balance, transaction history, personal loan and credit cards, investment holdings, and identity information. Throughout this report, we will refer to the client as Plaid.

Plaid is a private company, founded in 2013 by Zach Perret and William Hockey, located at San Francisco, California. Zach Perret, Co-founder of Plaid, explained that it was consumer needs that ignited the idea of safe and secure financial services. Now, Plaid is a company that is getting investments from American Express, Citi, Visa, and more financial corporates, and has grown to a company that has about 500 to 1,000 employees[1]. Key staff roles include CEO, Chief Legal Officer, CTO, and IT Security[2].

Plaid headquarter is currently located in leased space, sharing the building with ONLYONEU at 1098 Harrison St., San Francisco, California, and its branches located in Canada, US, UK, and Europe. Plaid allows its employees to work from home and these roles include Software Engineers, CRA risk analysts, and more.

Plaid makes about $200 Million in annual revenue, with a profit margin of 20-25%. Their business is still growing as they are expanding their business into more financing services, and more customers flowing in. This indicates that their data is becoming bigger and richer creating a better environment and infrastructure for users and customers[3].

Plaid utilizes secure cloud to build its safe infrastructure and to host its API. Security researchers and financial institutions such as Schellman, Doyensec, and TruSight, regularly audit Plaid's API and security controls and are continuously monitored by its own information security team. Plaid also protects their infrastructure by requiring multi-factor authentication for added security. Plaid allows users to customize their integration by allowing users to access its API. They also have a community on hackeron.com, which allows ethical hackers to help find and fix vulnerabilities in a system before they can be exploited.

Plaid uses a chat bot to serve customers on their website, leading to customer service. They rely on Google as its regular email and business communications (See Figure 2 in Appendix A for reference). Its web server runs on the latest version of AWS with regular updates. Plaid hosts 4 other servers in case their server goes down (See Figure 1 in Appendix A for reference) and will

---

[1] Crunchbase report on Plaid: https://www.crunchbase.com/organization/plaid
[2] Plaid Organization Chart: https://www.theinformation.com/org-charts/plaid
[3] Plaid Security Description: https://plaid.com/what-is-plaid/

still be performing normal business operation. Plaid also utilizes an anti-DDoS managed service AWS Shield to protect better against DDoS. Users will be able to login to access services due to the several servers hosted, unless all four servers go down due to an unforeseen event, or the company server that implements Plaid API goes down. In addition, Plaid holds International Organization for Standardization (ISO) certificate 27001, issued by Schellman. Their website implements TLS 1.3 cipher suites, AEAD-AES128-GCM-SHA256.

Plaid Inc has corporate firewalls and AWS firewalls deployed for network security purposes and deployed a robust Intrusion Detection System to monitor unauthorized behavior in their infrastructure. Its Virtual Private Cloud is protected using AWS security groups. The corporation scans every email to prevent data leakage and to reduce the impact of spam and phishing attacks, and employees are trained for security awareness every one year.

Plaid review permissions for internal systems periodically to ensure that the principle of least privilege is maintained, while backing up their data on a daily basis and replicating across multiple regions for redundancy.

Plaid also has adequate ReCaptcha step-ups and AWS shield which is used to protect from excessive bot generated traffic. It stores all its infrastructure secrets in a secure Key Management Service. User credentials are salted, hashed, and stored encrypted before storage.

Employees at Plaid access internal systems protected by WebAuthN and use strong second factors such as Yubikeys or biometrics. Plaid assets and the information are granted on a “need to know” basis based on roles and responsibilities. Its employees do not have unrestricted access to Plaid assets and information beyond that which is needed for the performance of their jobs.[4]

[4] Information provided by Plaid Security Portal: https://security.plaid.com/

Qualitative Risk Analysis

In assessing the risks for Plaid, I identified five major areas of cybersecurity concerns:

- Risk of cloud server being down via insiders, misconfiguration, or attack
- Loss of user payment information, user credentials, and transaction records via insiders, misconfiguration, or attack
- Loss of intellectual property such as encryption methods, and API via insiders, misconfiguration, or attack

Assets

Plaid's physical assets include all the materials, systems, and equipment located at their headquarter in San Francisco, and other branches including desktops, phones, printers, and more.

Plaid's information assets include user credentials, such as username, passwords, date of birth, their paystubs that they submitted for verification, phone numbers, user payment information, such as credit card number, emails, backend database and user transaction records. All the information is stored on a cloud server with copies being made available and backed up on a daily basis.

Looking at the structure of Plaid operation, the majority of their business information is stored on a cloud server hosted by AWS. The API system connects the third parties with consumers, generating their revenues, requires the cloud server to be stable and available whenever they need and require it. While its data backup policy allows it to restore and recover in the event of server loss, they have no plans during the server down time due to unforeseen events.

Furthermore, intellectual property such as Plaid's encryption technology and API is also stored on a cloud server. While its API documentation is available for access to customers and users on their website, and codes available on its GitHub repository for users to customize their own apps, the security of it is in question. Communities like Hackerone.com have records of finding vulnerabilities in Plaid's API, but possibilities of zero-day exploitation lies when updates are made. This can result in data breaches and intellectual property theft.

Threat Vectors

For the cloud server, there are multiple sources of disruption. There are three major situations where a cloud server might lose power: DDoS attack, Cloud Ransomware, Insider, and misconfiguration. Internet connectivity can be disrupted by a Distributed Denial of Service, DDoS attack aimed at the server, cloud ransomware, and insider sabotage.

Risk of the data assets is the loss of confidentiality or integrity of user data via direct hacking, phishing, and insider espionage.

In looking at the means of compromise, one particular concern is that Plaid heavily relies on AWS for its web servers and cloud server, which had known vulnerabilities in the past: issue

with data.all which can enable user data extraction labeled as Medium with CVSS score 6.9, issue with AWS client VPN which can allow actors to execute commands with elevated permissions due to buffer overflow, labeled as Medium with CVSS score 6.7, issues with AWS Deployment Framework which allows actors to elevate their permission, labeled as High with CVSS score 7.8, and more. Click the hyperlink to see more of AWS vulnerabilities. These vulnerabilities allow actors to elevate their privileges, and to potentially execute malicious commands to disrupt the server and access data assets including user information and Plaid's intellectual property. These vulnerabilities have Exploitation Prediction Scoring System (EPSS) scores of 0.04% for 30 days probabilities of exploitation, and Exploitability Score between 0.8 to 1.8. This calculates to 0.48% chance of exploitation over the year for direct hacking.

It is known to have approximately 4% of DDoS attack being carried out yearly[5], and 13% of Ransomware attacks being carried out targeting small to medium companies in the last five years[6]. Collectively the risk of server shutdown is 17% per year. Because Plaid has a well-functioning cybersecurity team and follows strict cybersecurity practices, the percentage will be brought down by about 10%.

For data assets, the methods for gaining access to either user credentials, payment information or transaction records depends on vulnerabilities in the existing cloud infrastructure or insider espionage. Such losses would be captured in the existing risk for hacking and insider action and be estimated at approximately 83%[7]. However, Plaid's strong background check might bring down this percentage to 20%.

Threat Actors

Plaid is most likely to be the victim of criminal groups, or script kiddies who are looking to access its users' sensitive data for financial gain. An individual may be able to exploit vulnerabilities to its servers, but it would take time and be hard as an individual level to hack into Plaid's well monitored security.

Plaid is very likely to be the target of state sponsored actors and high-end criminal groups, as the information and system will be likely to be of their interest.

Losses

The first set of losses are connected to disruption of the platform service due to loss or compromise of the server. Based on analysis of Plaid financial reports, the company will lose around $100K per day if the users are not able to connect to its platform. If the server downtime is short, less than 48 hours, the possibility of loss would be reduced as the users may try again once the server is restored. Beyond 48 hours, the losses will come into play, being estimated around $500K a week, adding $100K per day. In addition, server restore fee would be

[5] Statistics for DDoS attacks: https://blog.cloudflare.com/ddos-threat-report-for-2024-q2/
[6] Statistics for Ransomware attacks: https://www.varonis.com/blog/ransomware-statistics
[7] Statistics for Insider Threats: https://securityintelligence.com/articles/83-percent-organizations-reported-insider-threats-2024/

necessary costing them between $100 to $300 per hour to recover the server, which takes 2 to 10 hours depending on the issue.
Secondary losses resulting from the disruption of the platform service might come from lawsuits from third parties that provide Plaid services, such as Venmo, and Betterment. Plaid already has partnerships with Meredith Fuchs and is building its own corporate law team within its Policy, Risk, and Legal Group. Estimated loss for this scenario would be $2M for settlement for a company, and potentially $20M if there are multiple lawsuits. In addition, Plaid will start losing its users and third parties if the outage is extended, potentially losing 15% of the users. This would be translated into loss of future revenue of up to $7.5M.

Another set of losses are connected to loss of intellectual properties, such as their encryption methods. There would be no direct loss in this scenario, as its cloud server is being replicated and backed up daily. However, there would be a secondary loss due to the loss of its reputation, and alternative services would be available to users. This will result in a loss of future revenue up to $5M due to potentially losing up to 10% of the users.

Lastly, a final set of losses are connected to the loss of user data, such as personally identifiable information, user payment information, and user transaction records. There would be no direct loss in this scenario. However, it would require the corporation to pay settlements for the lawsuits. This would be estimated to be $10M. In addition to the settlement fees, Plaid might face from regulators, which can be up to 4% of the company's global annual revenue or €20M, and between $100 to $50K per violation. The loss in this case is calculated as approximately $50M. Plaid might also lose up to 30% of its users due to the damaged reputation, losing future revenue of approximately $15M. Collectively, secondary loss in this scenario would be $65M

Scenarios

The chart below converts major losses described above.

Asset	Threat Methods	Threat Actors	Loss Types	Loss Scale
Cloud Server	DDoS Cloud Ransomware Insider Sabotage Misconfiguration Total Annual Probability of Occurrence: ~15%	Script Kiddies Criminal Groups Individuals State Sponsored Actors Insider	Loss of revenue Cost to restore if backups were affected Scales larger with length of down time Secondary loss from lawsuit and user leaving	Min $100K/day offline Recover: $100-$300/hr (2-10hrs) Est. of direct loss of $300K Legal fees & settlement: $5M - $20M Loss of future revenue due to leaving users: $1M - $7.5M
User Data	Direct Hack Phishing Insider Espionage Total Annual Probability of Occurrence: ~20%	Criminal Groups Individuals State Sponsored Actors Insider	Loss of payment records Secondary loss from lawsuit Loss of future revenue	Legal fees & settlement: ~$50M Loss of future revenue due to leaving users: $15M
Intellectual Property	Direct Hack Phishing Insider Espionage Total Annual Probability of Occurrence: ~10%	Criminal Groups Individuals State Sponsored Actors Insider	Loss of competition in market Loss of future revenue	Loss of future revenue due to leaving users: $5M

Table 1. Scenario Chart.

Scenario 1 – Loss of Server

The risk of loss of the server due to cyberattack or insider sabotage is assessed appropriately at 15% per year. Cyberattacks targeting server is known to be 9% and in North America, main attack type was ransomware with 30% of attacks[8]. Taking insider sabotage probability into account, and Plaid's strong cybersecurity configuration, the actual server compromise or attack by external and internal actor is assessed at 15% per year. The estimated direct loss from this scenario ranges from $300K to $700K, and secondary loss ranges from $5M to $20M due to regulatory fines, settlement, and loss of future revenue due to lost customers.

Scenario 2 – Loss of User Data

The risk of loss of user data, including PII, user payment information, and transaction records, is assessed appropriately at 20% per year. Cyberattacks targeting user data is known to be nearly half, 46%, of breaches[9]. Insider espionage is taken into consideration with the security level of Plaid, calculating the risk assessment to 20% per year. There are no direct losses in this scenario, but it would require Plaid to pay legal fees and lose future revenue. Here, settlement is estimated of $10M and up to $50M, and regulatory fine of 4% of global annual revenue ($8M), regulatory fines of $100 to $50K per violations, and future revenue loss of $15M due to 15% decrease in user, collectively ranging from $11M to $65M. Plaid is likely to be the target of state sponsored actors and criminal groups due to the size and the value of data they maintain.

Scenario 3 – Loss of Intellectual Property

The risk of loss of intellectual property is assessed at 10% per year based on the collective hacking risks across Plaid IT systems. There is no direct loss calculated in this scenario, as cloud storage will allow them to recover their data without any cost, and it would not impact its revenue and daily operations. Secondary losses would be loss of future revenue due to the loss of 10% of its customers. This ranges from $5M to $20M, as customers and users may think it is less severe than user data breach. However, Plaid's reputation may be damaged and in the long run, alternative services will be available for users, providing them with similar services.

[8] https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=In%20Asia%2C%20the%20main%20attack,in%2021%25%20of%20attacks).

[9] https://secureframe.com/blog/data-breach-statistics

This is a heat map of each scenario which captures them in terms of probability and impact.

Certain				
Very Likely				
Likely				
Unlikely			Scenario: Loss of Server	Scenario: Loss of User PII, and Data
Possible		Scenario: Loss of Intellectual Property		
Probability vs. Severity	Low	Medium	High	Severe

Table 2: Heat Map

Scenario: Loss of Server is placed in unlikely, which serves 10% to 35% range, and high severity. As indicated as the color, it is in the yellow zone, which indicates just a warning.

Scenario: Loss of User PII, and Data is placed in unlikely, but is placed in severe. This is due to the fact of the great amount of potential loss.

Scenario: Loss of Intellectual Property is placed in possible, which serves 10% or less, and medium severity. As indicated as the color, it is not as dangerous as others, but still should be aware of potential attack, and its damage.

Quantitative Risk Analysis

As mentioned above in the Qualitative Risk Analysis, Scenario 1 covers the range of possible events that could result in the loss of cloud server. This includes attacks, insider sabotage, and misconfiguration, which results in the unavailability of the platform service, losing the ability to generate revenue.

Pre-mitigation Loss Analysis for Scenario 1 – Loss of Server

Minimum probability 5%, Most likely value 15%, and Maximum chance of 20% were used as the basis of vulnerability, and frequency of occurrence will use values of 0.75 to 2.5; Minimum 0.75, Most likely 1.25, and Maximum 2.5.

Figure 1-1. Probabilities for Scenario 1

Direct loss of productivity ranges from $300K to $700K, with Most likely value of $450K, and response cost ranging from $100 to $3K, with Most likely value of $300.

Secondary losses of productivity ranges from $1M to $7.5M, and is most likely be $2M, with 20% of probability of occurrence, and settlement fee between $5M to $20M, and most likely value of $12M with also 20% of probability of occurrence. Overall, the probability of secondary losses ranges from 10% to 40%, with most likely value of 20%.

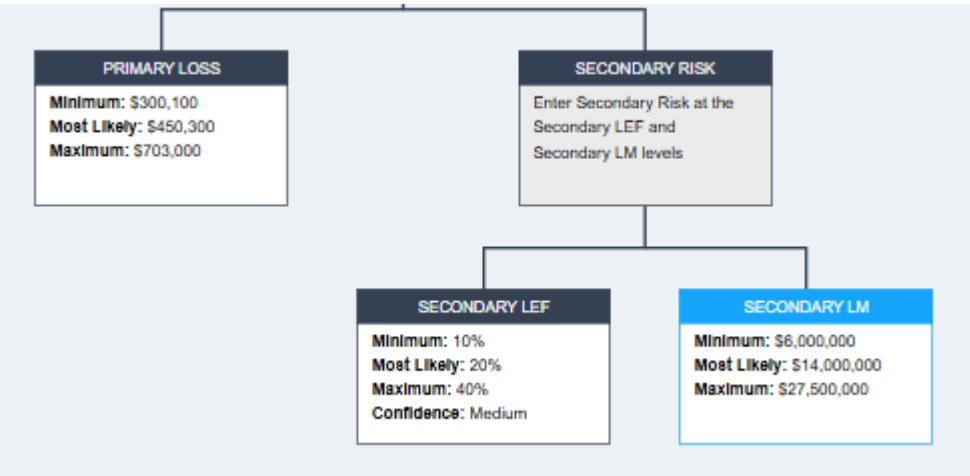

Figure 1-2. Loss Values for Scenario 1

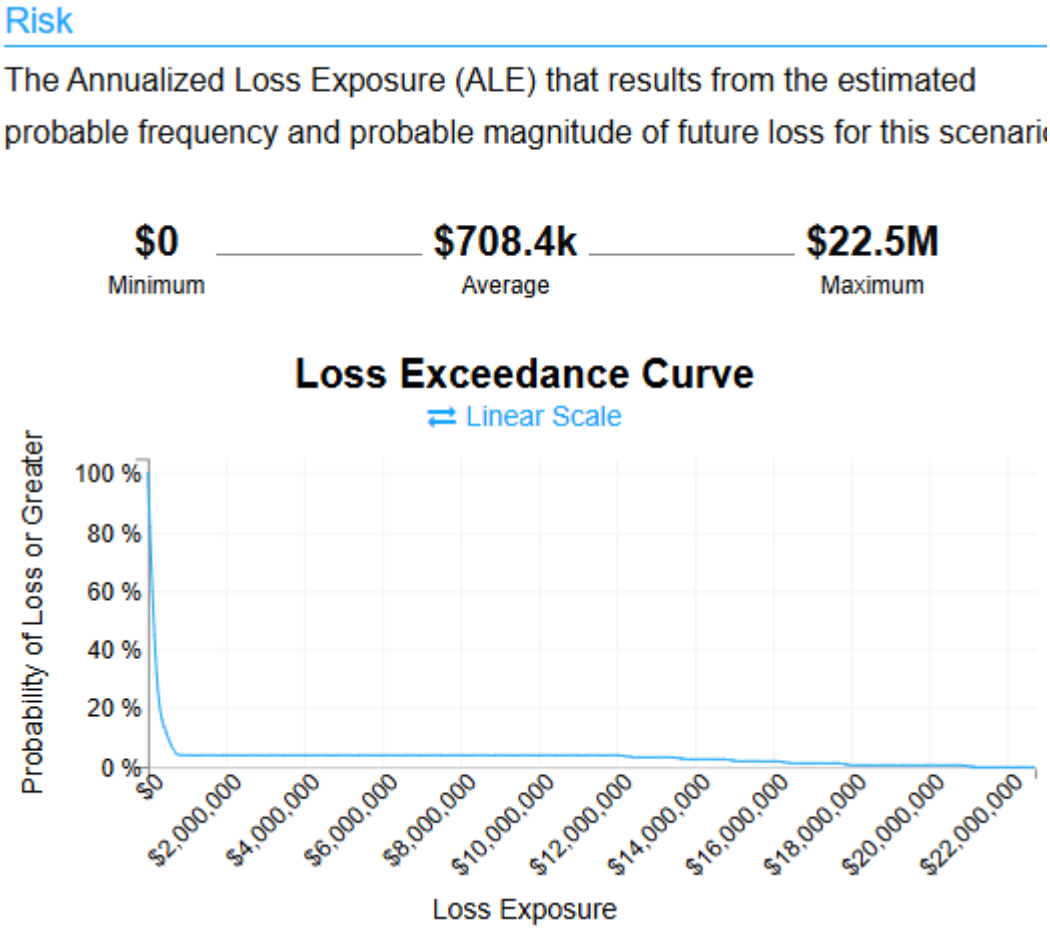

Figure 1-3. Pre-Mitigation Loss Exceedance Curve

100% Discounted Loss = 1 x 0 = 0
20% Discounted Loss = 0.15 x 708,400 = $106,260
1% Discounted Loss = 0.01 x 55,500,000 = $225,000
Expected Loss = $331,260

Based on the calculation, Plaid's expected annual loss is $331,260, with contributions from both high-probability moderate losses (15% at $106,260) and low-probability catastrophic losses (1% at $225,000). To address these risks, we recommend Plaid allocate $300K toward server security. This amount strikes a balance between mitigating high-impact, low-probability events and addressing moderate, more likely risks.

While this does not entirely eliminate all risk, it represents a cost-effective approach that significantly reduces expected losses. Additional measures, such as insurance or further mitigation for the 15% scenario, can provide a safety net for residual risks.

Pre-mitigation Loss Analysis for Scenario 2 – Loss of User PII and data

Minimum probability 10%, Most likely value 20%, and Maximum probability 25% were used as the basis of vulnerability, and frequency of occurrence will use values ranging from 1 to 2.5, with most likely value of 1.75.

Figure 2-1. Probabilities for Scenario 2

There is no direct loss linked to this scenario.

Secondary losses of productivity ranges from $1M to $15M and $5M as most likely value, with 20% of probability of occurrence, and settlement and regulatory fine fees between $10M to $50M and $20M as most likely value, with 35% of probability of occurrence. Overall, the probability of secondary losses ranges from 20% to 60%, and 30% as the most likely value

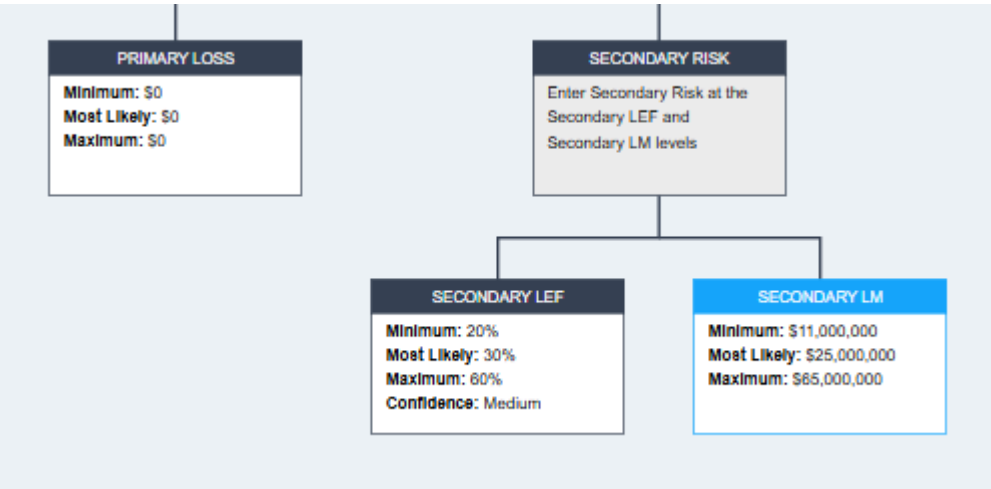

Figure 2-2. Loss Values for Scenario 2

Risk

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

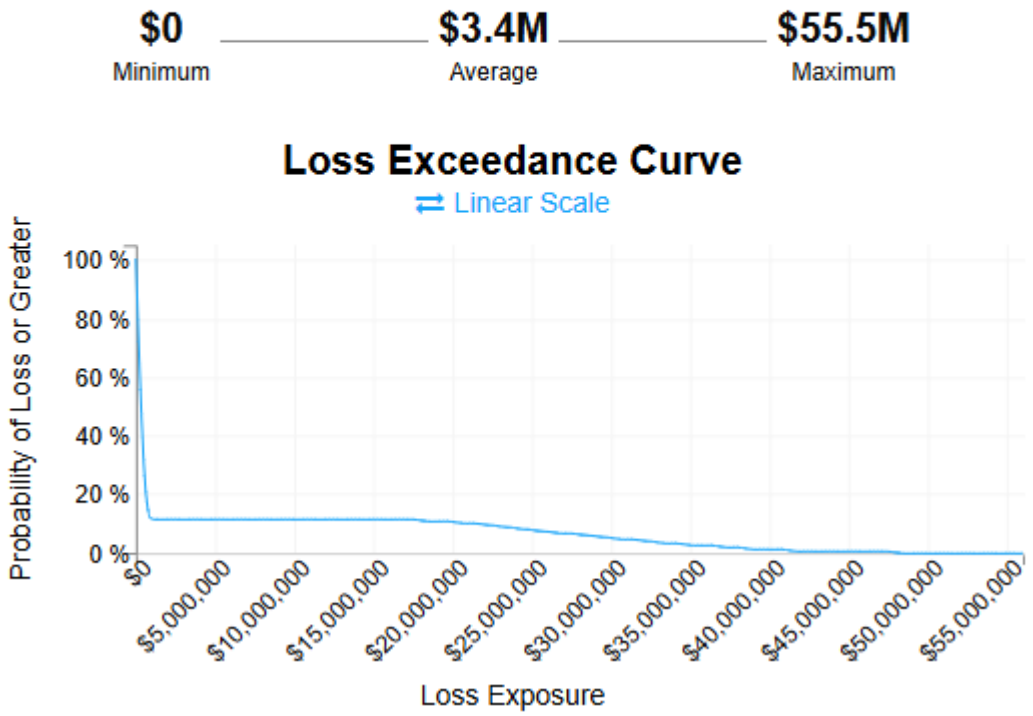

Figure 2-3. Pre-Mitigation Loss Exceedance Curve

100% Discounted Loss = 1 x 0 = 0
20% Discounted Loss = 0.2 x 3,400,000 = $680,000
1% Discounted Loss = 0.01 x 55,500,000 = $555,000
Expected Loss = $1,235,000

Based on the calculation, Plaid's expected annual loss is $1,235,000, with contributions from both high-probability moderate losses (20% at $680,000) and low-probability catastrophic losses (1% at $555,000). To address these risks, we recommend Plaid allocate $1M toward user data security. This amount strikes a balance between mitigating high-impact, low-probability events and addressing moderate, more likely risks.

While this does not entirely eliminate all risk, it represents a cost-effective approach that significantly reduces expected losses. Additional measures, such as insurance or further mitigation for the 20% scenario, can provide a safety net for residual risks.

Pre-mitigation Loss Analysis for Scenario 3 – Loss of Intellectual Property

Minimum probability 2%, Most likely value 10%, and Maximum probability 15% were used as the basis of vulnerability, and frequency of occurrence will use values ranging from 0.5 to 1.5, with most likely value of 1.

Figure 3-1. Probabilities for Scenario 3

There is no direct loss linked to this scenario.

Secondary losses of productivity range from $500K to $5M and $1M as most likely value, with 15% of probability of occurrence. The probability of secondary losses ranges from 5% to 15%, and 10% probability is the most likely value.

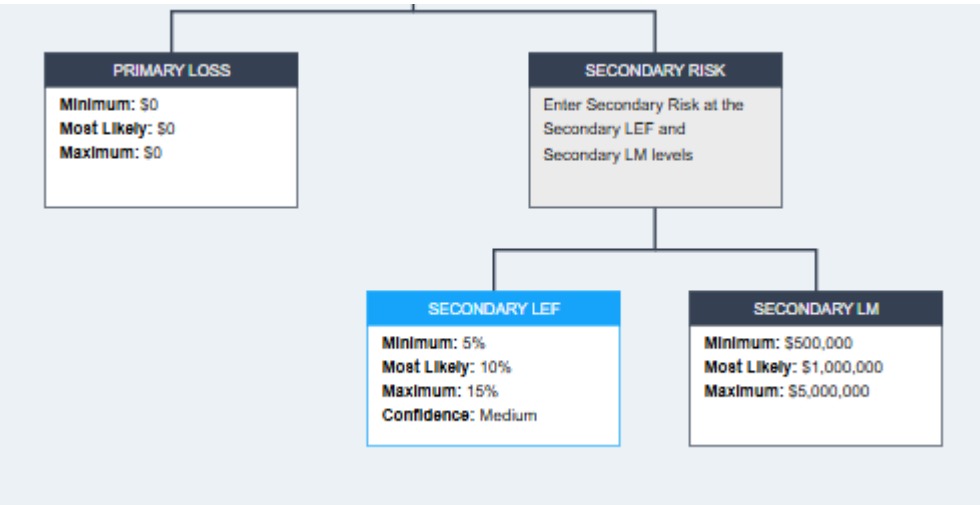

Figure 3-2. Loss Values for Scenario 2

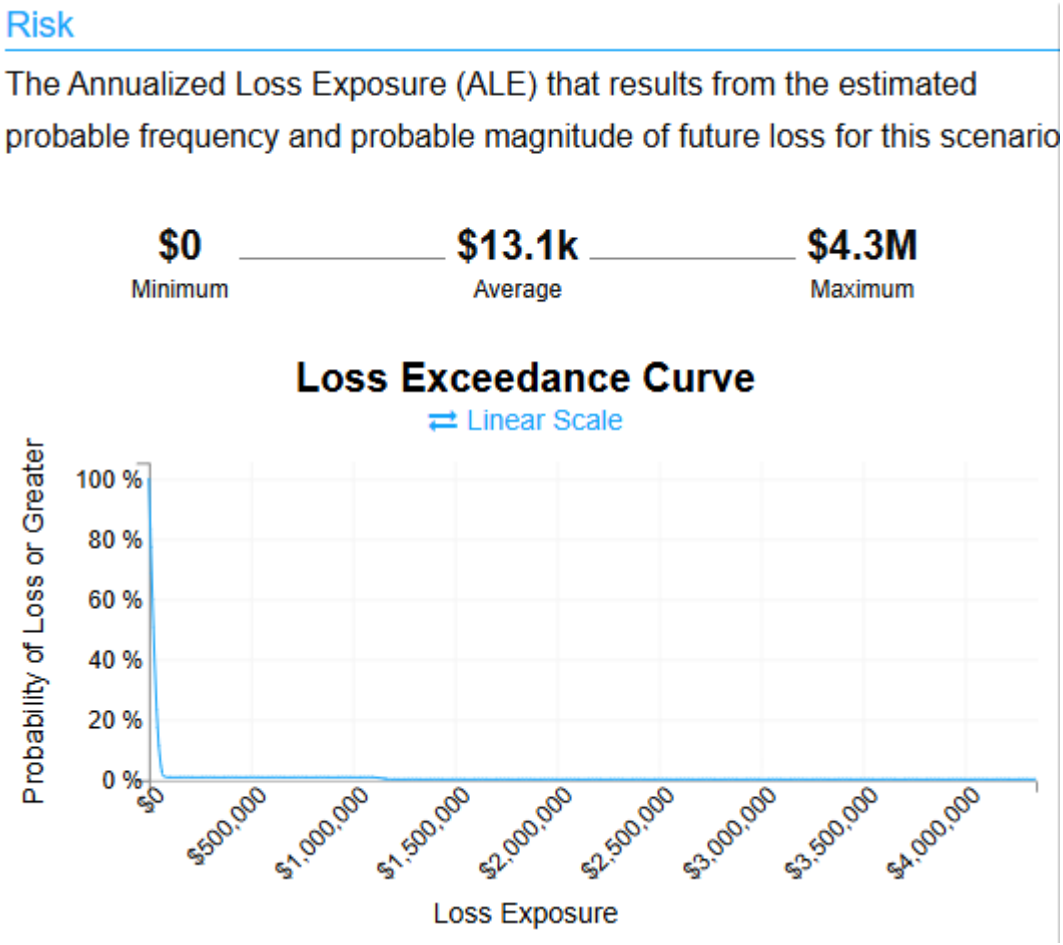

Figure 3-3. Pre-Mitigation Loss Exceedance Curve

100% Discounted Loss = 1 x 0 = 0
15% Discounted Loss = 0.15 x 13,100 = $1,965
1% Discounted Loss = 0.01 x 4,300,000 = $43,000
Expected Loss = $44,965

Based on the calculation, Plaid's expected annual loss is $44,965, with contributions from both high-probability moderate losses (15% at $1,965) and low-probability catastrophic losses (1% at $43,000). To address these risks, we recommend Plaid allocate $40K toward intellectual property security. This amount strikes a balance between mitigating high-impact, low-probability events and addressing moderate, more likely risks.

While this does not entirely eliminate all risk, it represents a cost-effective approach that significantly reduces expected losses. Additional measures, such as insurance or further mitigation for the 20% scenario, can provide a safety net for residual risks.

Post-mitigation Loss Analysis for Scenario 1 – Loss of Server

By building redundancy in the cloud server, strengthening the monitoring process, optimizing website performance, implementing security measures and improving employee training on security awareness (which will cost less than $300K), Plaid can eliminate 5% per year risk related to the loss of cloud server, whether it is misconfiguration, or an attack. New baseline probability drops to 0.75%, but all other values remain the same.

Baseline probability 0.75%, Minimum value 0.5%, Most likely 0.75%, and Maximum value 1%.

Figure 1-4. Post-mitigation probabilities for Scenario 1

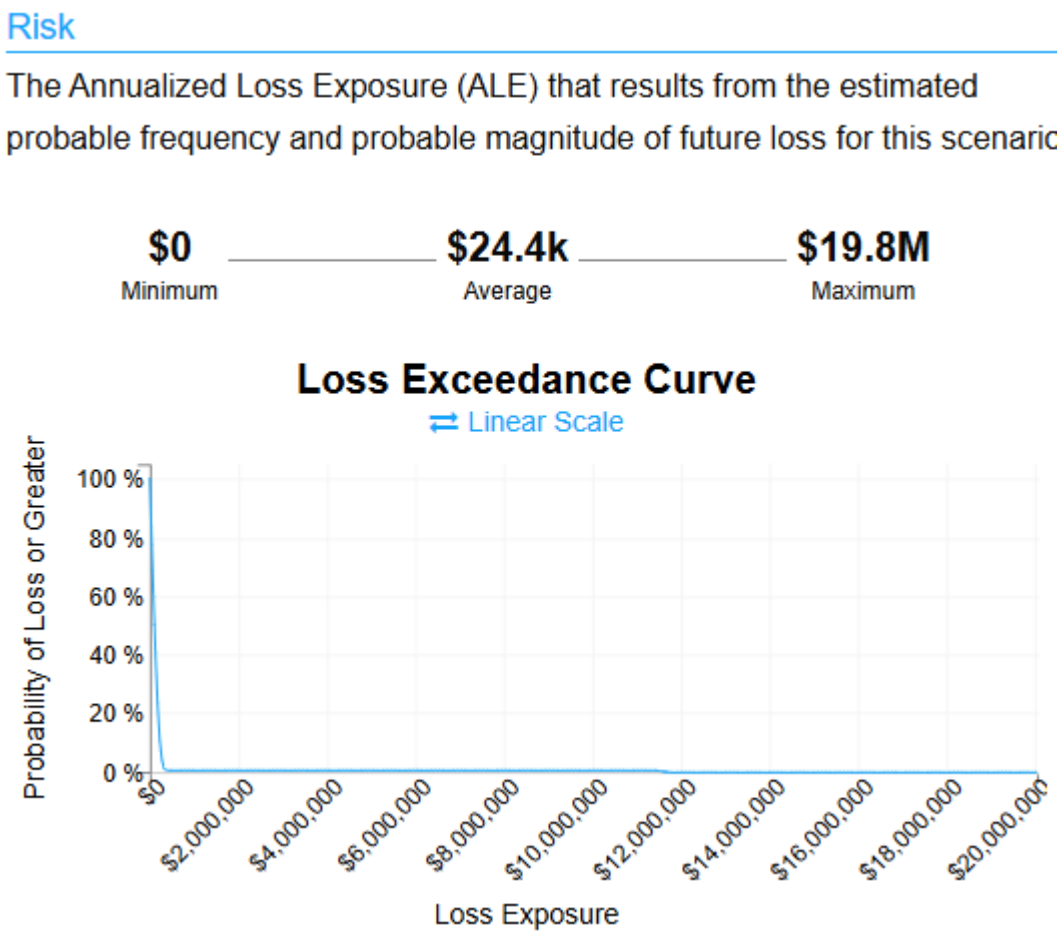

Figure 1-5. Post-mitigation Loss Exceedance Curve

By implementing stronger security around the server, the annual average risk of loss drops from $708.4K to $24.4K, which is about 97% decrease, and maximum drops from $22.5M to $19.8M. Implementing strong security around the server has brought significant changes from pre-mitigation loss analysis.

Post-mitigation Loss Analysis for Scenario 2 – Loss of User PII

Implementing strong tool for user data security, conducting more regular vulnerability assessment, providing employee training on phishing attacks, and implementing a strong security for database will cost Plaid around $1M but will eliminate 7% per year risk related to the loss of user data. New baseline probability drops to 0.9%, and all other values remain the same.

Baseline probability 0.9%, Minimum value 0.3%, Most likely 0.9%, and Maximum value 1%.

Figure 2-4. Post-mitigation probabilities for Scenario 2

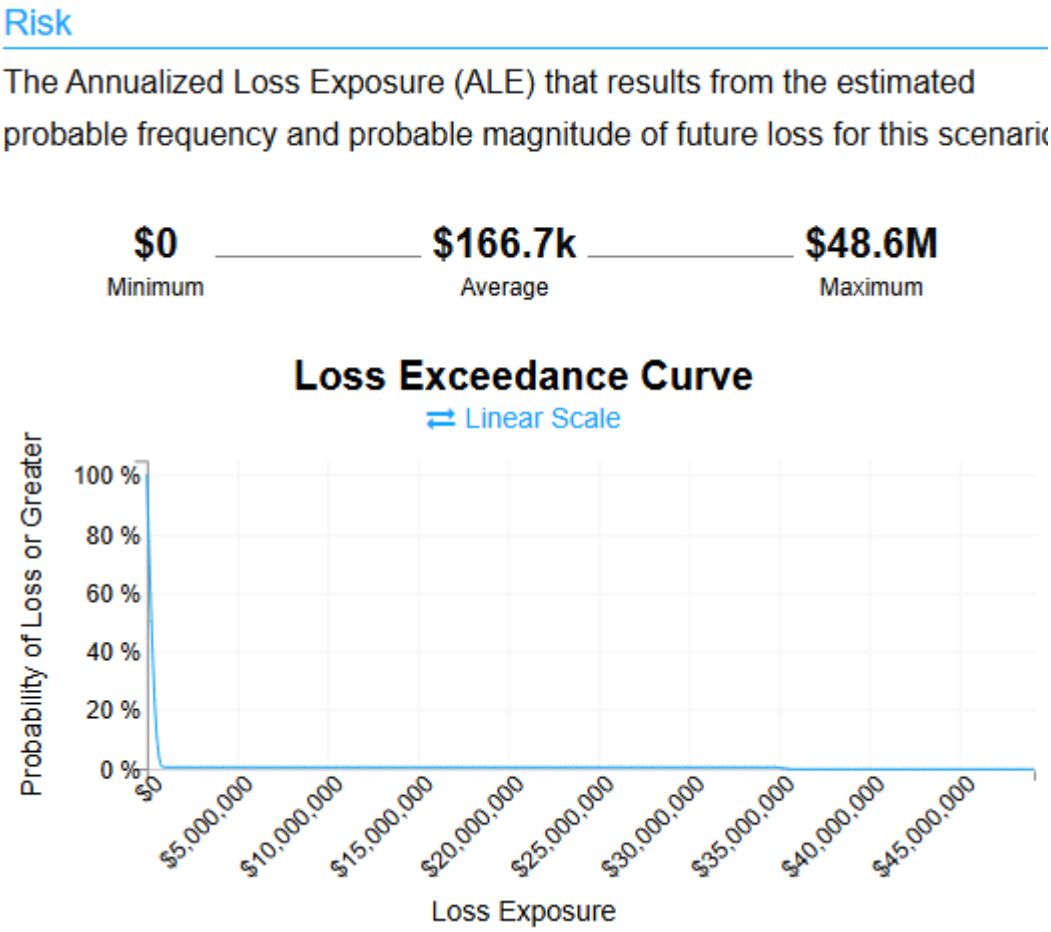

Figure 2-5. Post-mitigation Loss Exceedance Curve

By implementing stronger security around the user PII and data, the annual average risk of loss drops from $3.4M to $166.7K, which is about 95% decrease, and maximum drops from $55.5M to $48.6M. Implementing strong security around the user data has brought significant changes from pre-mitigation loss analysis.

Post-mitigation Loss Analysis for Scenario 3 – Loss of Intellectual Property

Developing a strong tool to protect intellectual property, conducting more regular vulnerability assessment, and implementing a strong security for database will cost Plaid around $13.1K but will eliminate 3% per year risk related to the loss of intellectual property. New baseline probability drops to 0.3%, and all other values remain the same.

Baseline probability 0.3%, Minimum value 0.1%, Most likely 0.3%, and Maximum value 1%.

Figure 3-4. Post-mitigation probabilities for Scenario 3

Risk

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

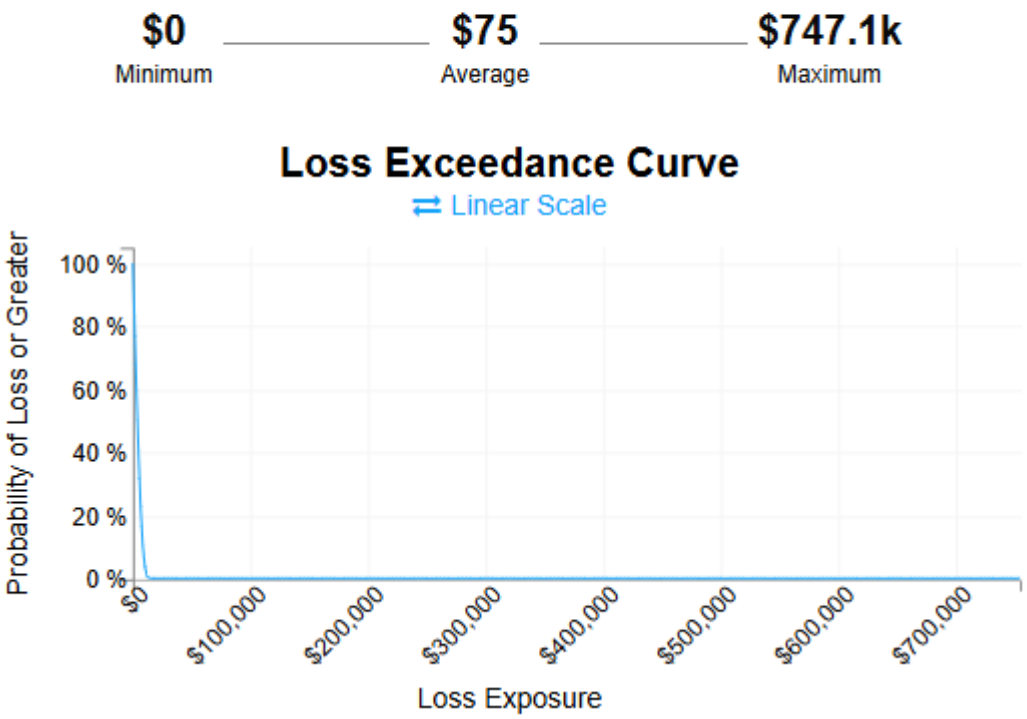

Figure 3-5. Post-mitigation Loss Exceedance Curve

By implementing stronger security around the intellectual property, the annual average risk of loss drops from $13.1K to $75, which is about 99% decrease, and maximum drops from $4.3M to $747.1K. Implementing strong security around the intellectual property has brought the most significant changes from pre-mitigation loss analysis.

Recommendations

Based on the analysis above, we have one critical cybersecurity recommendation to the board of Plaid, two highly recommended cybersecurity actions, and two suggestions for best cybersecurity practices. Total cost of these suggestions will not exceed $1.5M per year but will significantly decrease the risk of major loss events to around 10% risk per year of a $200K loss compared to now, which is likely to average $4.5M per year and around 15% probability per year of a $800K loss.

The critical cybersecurity recommendation for Plaid is to build stronger protection for the user PII and data by implementing strong tools for user data security, conducting more regular vulnerability assessment, and providing employee training. Ensure that all the software and hardware is updated, run penetration testing before updating their applications to prevent zero-day exploitation, and check for any vulnerabilities in your encryption algorithm. Creating defensive phishing campaigns is also necessary to test vulnerabilities against phishing. This will not only train the employees but also increase the awareness of phishing. Currently, 20% of some kind of attacks targets Plaid's user data per year and potentially leading to loss of as high as $55.5M. Reducing the danger and risks of attacks targeting the user data will reduce this probability to under 1% with significantly reduce in loss. Our recommendation is to make around $1M investment to protect user data and nearly eliminate the loss event.

Our two highly recommended cybersecurity actions will cost a total of $350K per year. This will contribute to better security, and to the domination of competition against other alternative services. The recommendations are to ensure that known vulnerabilities are patched as soon as possible in order to prevent unauthorized authorization to prevent any data breaches, and to implement a strong protection on the server. These activities will reduce the baseline risks for events of loss of server and intellectual property by around 1% per year to 0.5% per year. These activities will help minimize the extent of secondary losses by enabling Plaid to showcase a strong cybersecurity program when responding to legal actions stemming from any future incidents. The $350K investment in these areas will significantly reduce the potential losses from an average of $720K to $25K per year.

Lastly, we would encourage Plaid to polish their cybersecurity policies by setting a clear cyberattack protocol and implement a strong employee training to enhance resilience against business interruption events. Employee training can include phishing campaign, and simulation of attacks as scenarios provided above to minimize their loss and increase the awareness of cybersecurity.

Ciprian IT suggests that corporates should spend about 6% of their annual revenue (Ciprian IT, 2024). This indicates that disregarding the size of business, any businesses should spend at minimum 6% of their annual revenues for cybersecurity, which converts to 5-20% of IT security budgets.

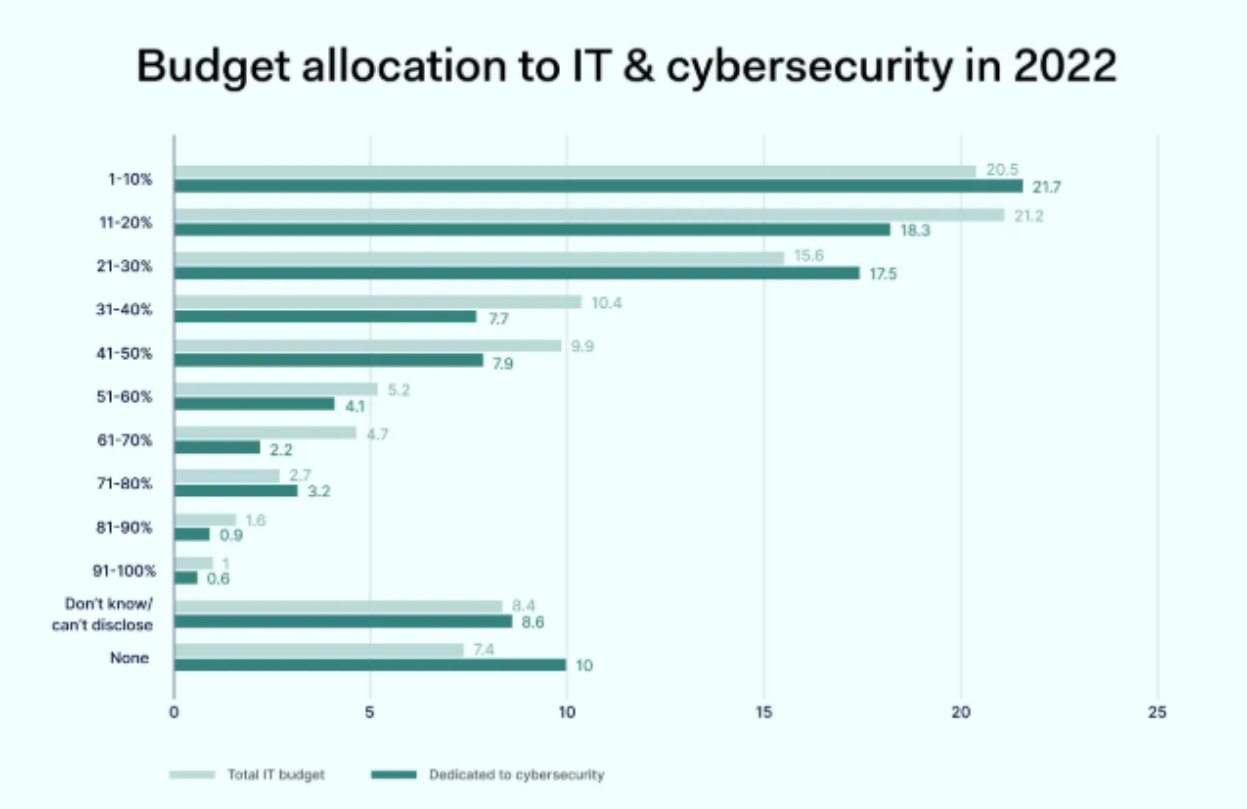

Figure 4. https://nordlayer.com/blog/best-practices-cybersecurity-budget-research-guide/

As the graph indicates, nearly one-fifth of organizations allocated 30% of their budget to cybersecurity. This trend continues to grow as data sensitivity and security become increasingly important.

Appendix A

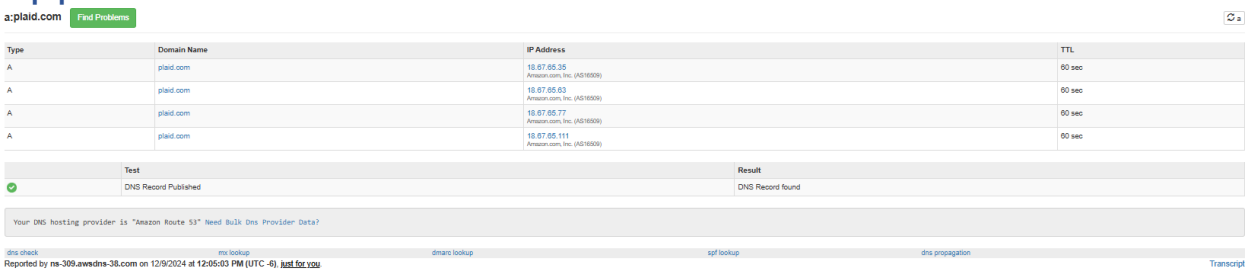

Figure 1

This is the result of DNS lookup on MxToolBox. This indicates that Plaid, has multiple servers running with IP addresses: 18.67.65.35, 18.67.65.63, 18.67.65.77, and 18.67.111. They are powered by Amazon.

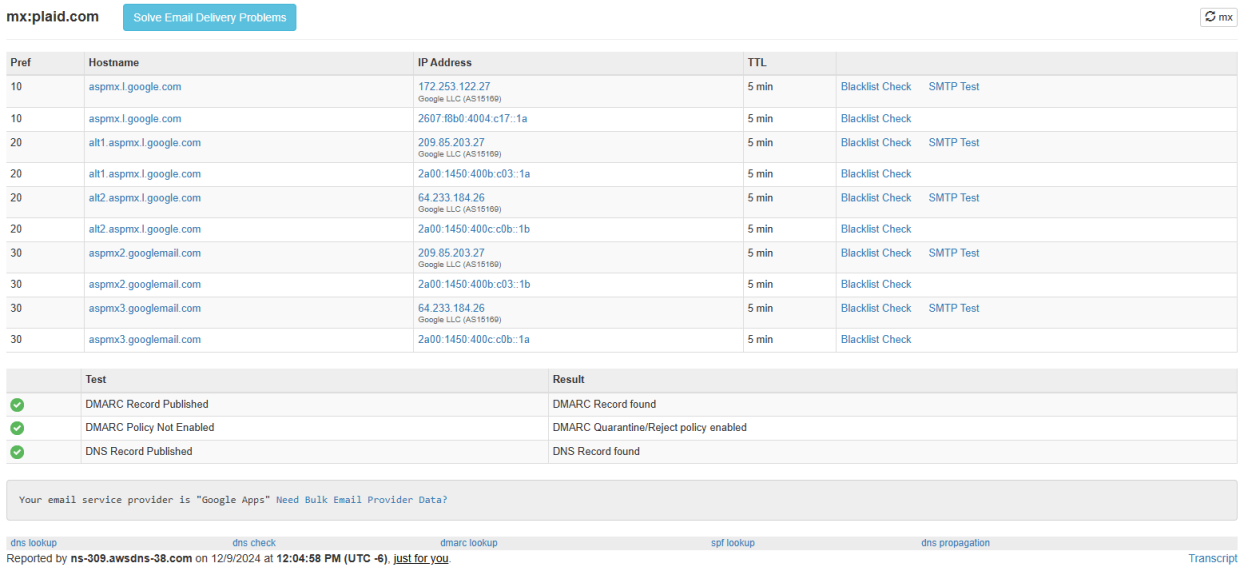

Figure 2

This is the result of MX lookup on MxToolBox. This indicates that Plaid uses google for their email services and operates both on IPv4 and IPv6.

References

Ciprian IT. (2024, April 23). *How much should my business spend on cybersecurity?*. How Much Should My Business Spend on Cybersecurity? https://www.linkedin.com/pulse/how-much-should-my-business-spend-cybersecurity-ciprianit-yswhe/

Smart, J. (2021, March 15). *Plaid's journey from idea to Fintech powerhouse*. Silicon Valley Bank. https://www.svb.com/industry-insights/fintech/plaids-journey-from-idea-to-fintech-powerhouse/