NormShield

2020 NormShield Financial Risk Report

An in-depth financial third-party risk analysis of US Financial Institutions

Attacks toward the Financial Sector on the rise

Cybercriminals pose as FINRA executives

According to the Boston Consulting Group's recent study, the financial sector has been hit 300 times more than any other industry sector, with the aftermath incurring a higher cost. Recent alerts from the Financial Industry Regulatory Authority (FINRA) support these findings, highlighting an ongoing email scam targeting the finance sector with the aim to usually steal usernames and passwords.

In the "ongoing" phishing campaigns, attackers impersonate FINRA executives, including Vice Presidents Bill Wollman and Josh Dubnyk.

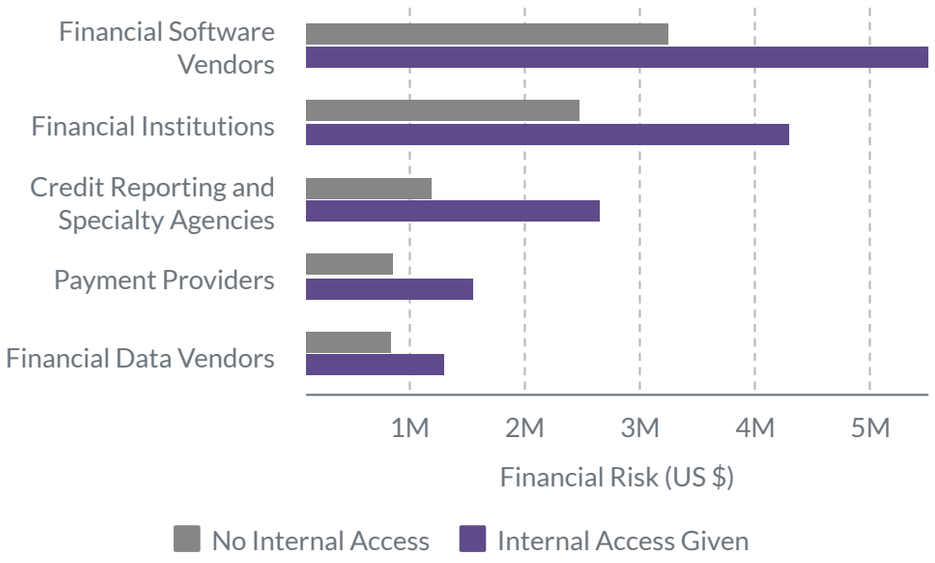
In this report you will find...

- Top third-party Financial Sector vendors across 10 different verticals
- Analysis of financial risk using comparable numbers of sensitive records shared
- How the risk fluctuates with or without internal access granted to the third party
- Average risk vs. maximum risk, and why it's important
- Steps to manage third-party risk

"The financial sector has been hit 300 times more than any other sector..." - BCG

SNEAK PEAK

Cyber Risk across the Top 5 Third-Party Vendors in Finance



For 500,000 records

The finance sector is known to house large amounts of sensitive information, which is often harvested once an attack becomes successful. As such a rich source for data, attackers are lured to the Financial Ecosystems, if not to the banks themselves.

Threat actors hoping to find cracks in an ecosystem usually hit third parties to harvest information, hoping to lead them to larger organizations. The effect of a cyber event quickly multiplies in an ecosystem, even creating a ripple effect and extending to other victims.

What lures attackers to the Financial Sector?

- To exfiltrate financial information, including credit card numbers, CVVs, and card dates
- To exfiltrate personal information to sell on the dark web

- Immediate monetization through ransomware attacks

> Finance is a sector where massive amount of personal information could be harvested by hackers.

Financial Risk and FAIR

According to the FAIR Institute, risk is defined as "the probable frequency and probable magnitude of future loss" associated with a specific event. In simple terms, one can identify risk as the "probable loss" in a predetermined scenario.

A threat scenario, the affected asset(s), their value to the organization, and the possible consequences are indispensable elements in a risk discussion.

Knowing and understanding the third-party ecosystem and the risk is critical in a risk management process.

It is important that (third party) risk management professionals focus their limited resources on risky vendors. Knowing who presents a high probability and/or impact risk beyond the organization's risk appetite is critical, saving time-consuming assessments on a vendor who poses a low probability of financial loss or on vendors who pose little risk overall.

What is FAIR?

Factor Analysis of Information Risk (FAIR) is the only international standard quantitative model for information security and operational risk. The model:

- Provides an understanding, analysis, and quantifiable information on risk in financial terms
- Is unlike risk assessment frameworks that focus output on qualitative color charts or numerical weighted scales
- Builds a foundation for developing a robust approach to information risk management

The Open FAIR model components are specifically designed to support risk quantification, through:

- A standard taxonomy and ontology for information and operational risk
- A framework for establishing data collection criteria
- Measurement scales for risk factors
- A modeling construct for analyzing complex risk scenarios

NormShield leverages the Open FAIR model to calculate the probable financial impact if a third-party vendor, partner, or supplier experiences a breach, and communicates risks in quantitative, easy to understand business terms.

OUR RESEARCH

NormShield identified the Top 20 U.S. Financial Institutions and their third-party vendors from various sectors to study the financial risks they are incurring due to cyber attacks

The sectors identified as the most common third-party vendors to financial institutions include:

First-Party Collections

Credit Reporting and Specialty

Financial Software

Financial Data Services

Identity and Technology Services

Interbank Network

Know Your Customer (KYC) / Anti-Money Laundering (AML)

Marketing

Payment Provision

Cyber Risk Across Third-Party Vendors in Finance

We identified the financial cyber risk for the Top 20 U.S. Financial Institutions along with their most common vendors.

The risks are calculated according to the average number of records financial institutions share with their vendors or each other, and also the internal access granted to these vendors.

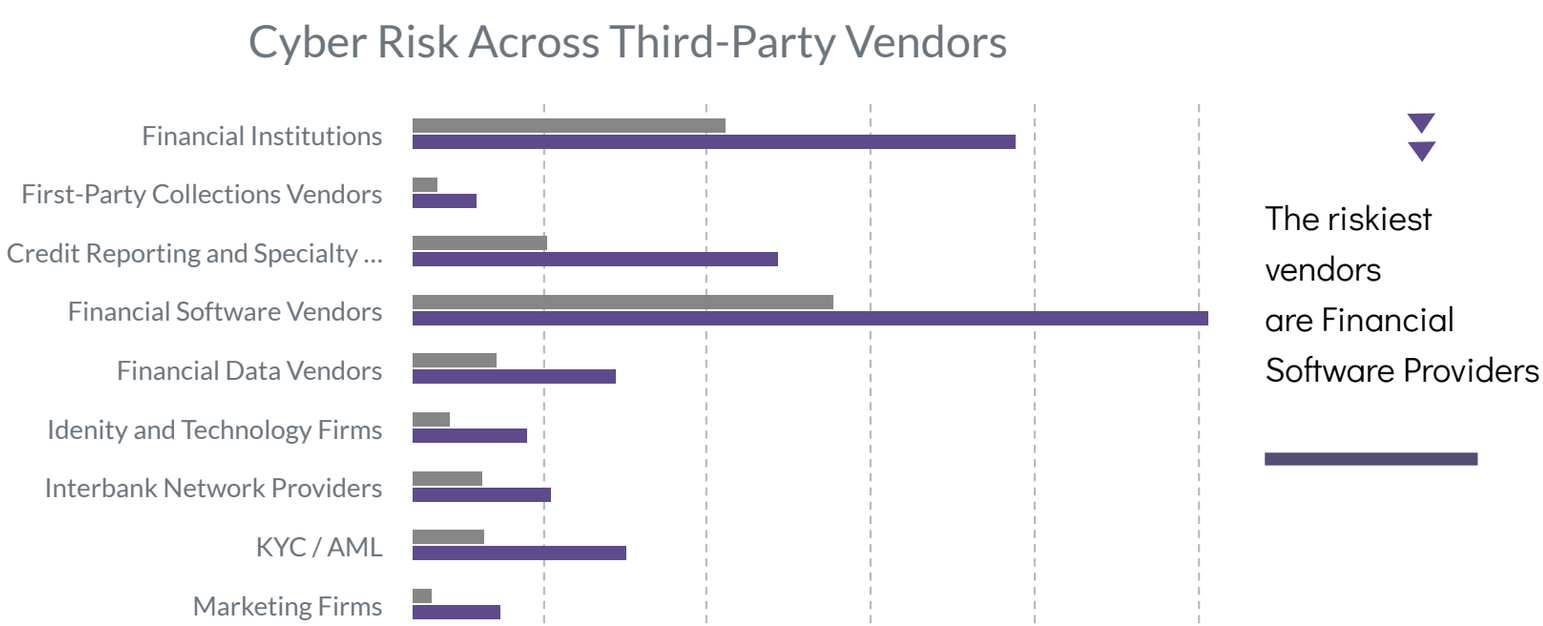
These records could be either Personally Identifiable Information (PII), Credit Card Data (PCI), or Protected Health Information (PHI).

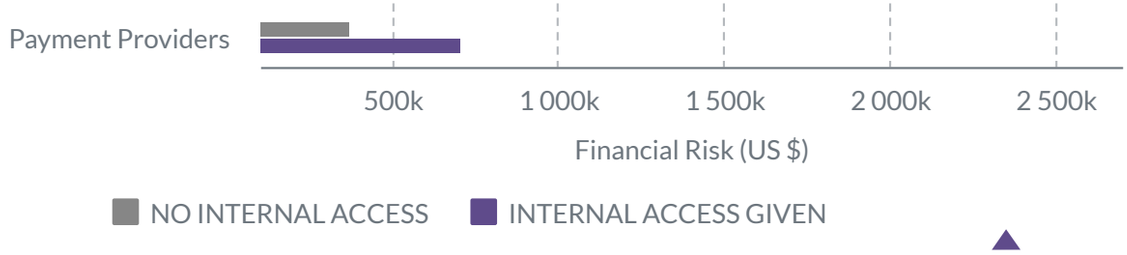
What happens when internal access is given to third-party vendors?

New partnerships and technologies change the access needs of the user. It is not uncommon for organizations to grant internal access to contractors, vendors, and other third parties. With internal access, corporate parameters are expanding and even becoming what some would call "blurry."

Several well-known security breaches have occurred by initial access to vendor systems followed by broader access to merchant systems, as was the case in the 2013 Target breach. Attackers invaded Target's network after hacking a third party vendor providing heating, ventilation, and air conditioning services. At the end of the day, the breach affected more than 60 million customers across 41 states in the U.S. and exposed to credit/debit card information of 40 million customers.

Ideally, internal access should only be activated on an as-needed basis and disabled when not in use.

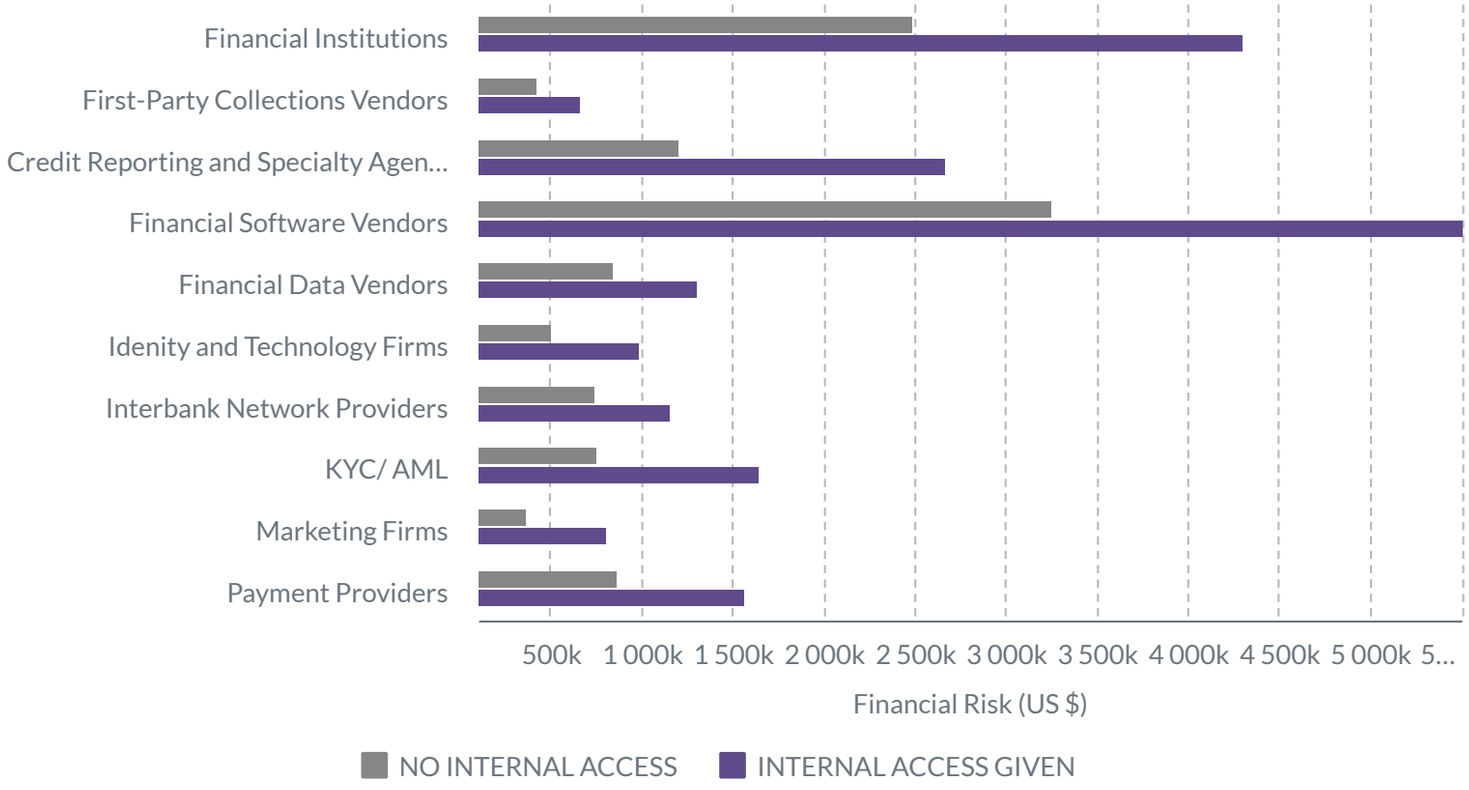




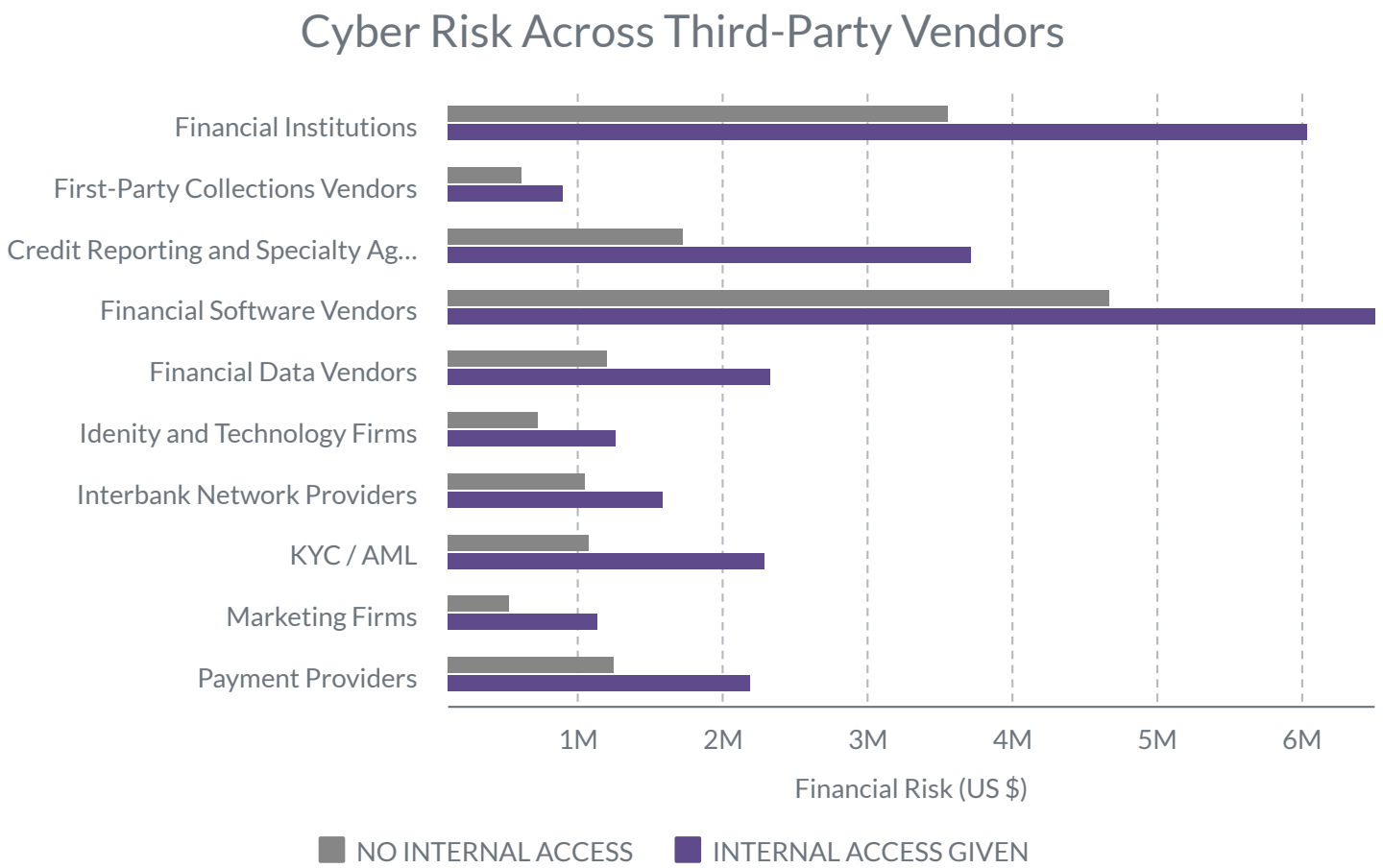
For 100,000 records

NormShield's utilizes the Open FAIR methodology along with data in the "The 2019 annual cost of a Data Breach Report," conducted by the Ponemon Institute and sponsored by IBM Security. This study analyzes data breach costs reported by 3,211 individuals within 507 organizations, across 16 geographies, and 17 industries. According to the findings, the average size of a data breach varies by country and industry.

Cyber Risk Across Third-Party Vendors



For 500,000 records



For 1,000,000 records

NormShield calculates risk using the number of records, the geography of the organization, and above all the external cyber security health of an organization.

The number of records shared is crucial in risk calculation as it stands as one of the key factors when determining the cost of a data breach.

Overall, shared records require employee time and effort to notify victims and investigate the breach, customer churn, reputation

How Many Records Do You Keep or Share with your vendors?

damage, as well as regulatory fines. Organizations are also obligated to report the number of records breached in a cyberattack to Data Protection and Enforcement Authorities.

The Riskiest Vendors in Finance

According to our study, the riskiest vendors in the finance sector are Financial Software Providers with a cyber-related financial risk average upwards of $3M for 500,000 records. Financial Institutions, occasionally serving as third parties to each other, are second in place. Not far behind are Credit Reporting, Specialty Agencies, and KYC / AML Vendors.

The Cyber Risk of the Top 5 Finance Vendors

In this section, we analyzed the average and maximum financial risk with various numbers of

Financial Institutions can make informed decisions on their vendor ecosystem based on the Open FAIR report.

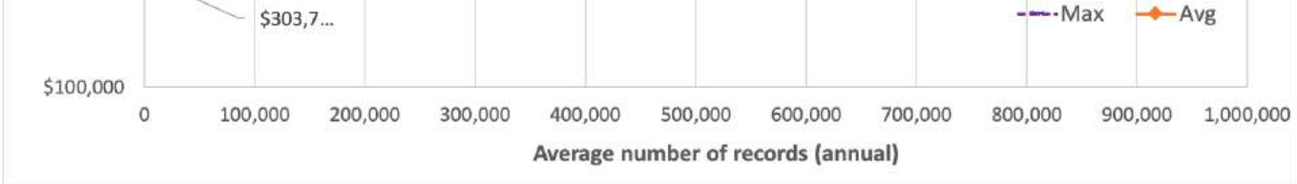
records shared. Based on NormShield data, as the number of records increases, the average risk changes on a logarithmic-like scale.

Costs incurred in a data breach, such as investigation costs, hiring of legal consultants, and reputation damage does not change in perfect proportion to the number of records shared.

Finally, as the maximum risk increases, the number of records shared increases as well. This spike is due to an unproportional increase in the maximum loss with regards to the average risk.

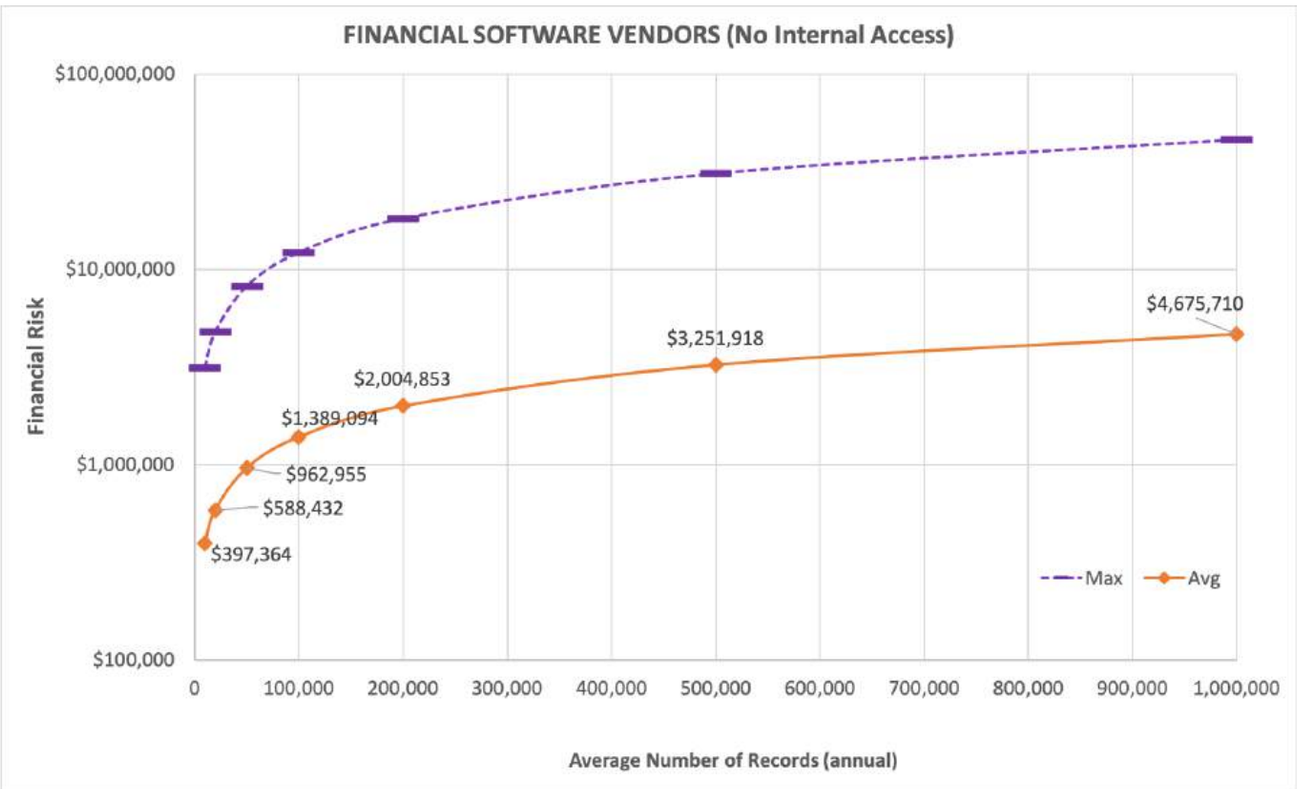
Financial Risk of Top U.S. Financial Institutions

Financial Institutions are most likely to be associated with a breach. Due to housing some of the most sensitive information, this sector incurs the highest maximum loss.

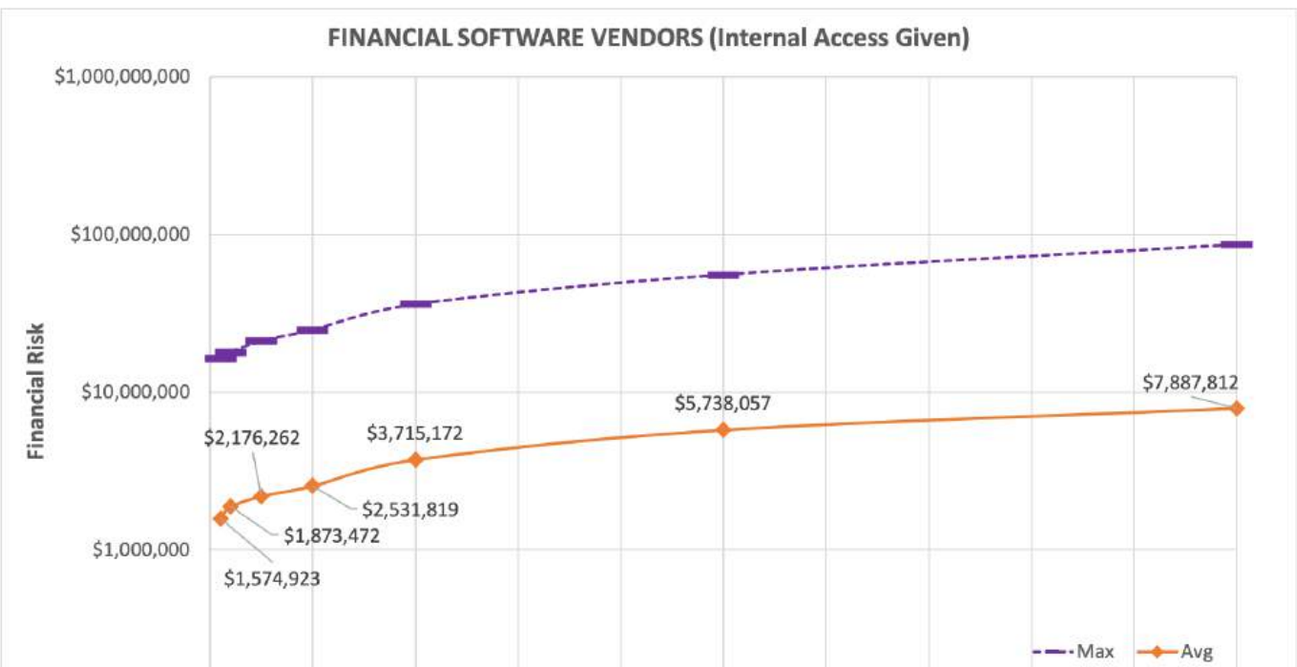


* Financial Risk axis is shown in logarithmic scale

Third-Party Financial Risk Caused by Financial Software Vendors



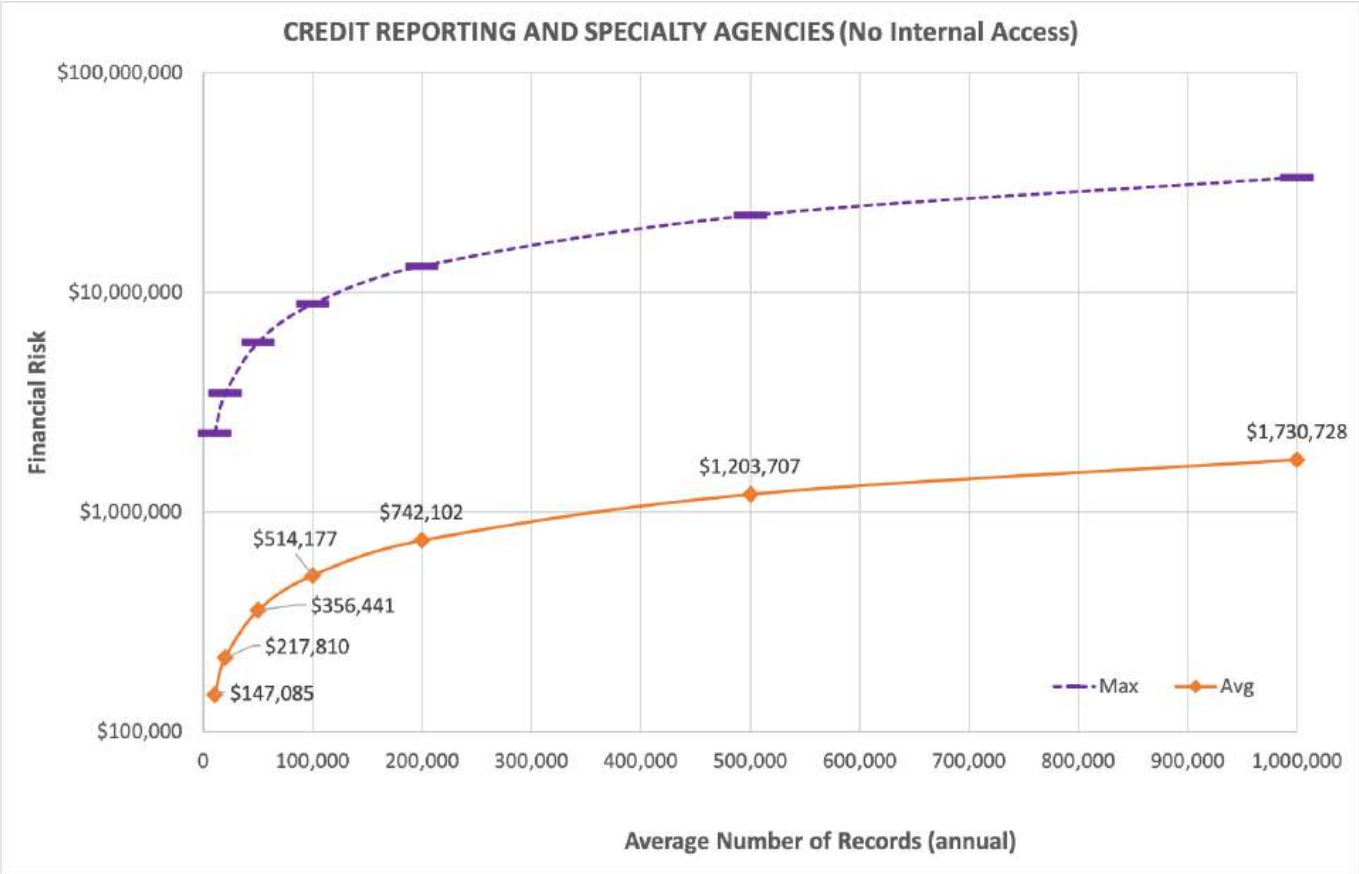
* Financial Risk axis is shown in logarithmic scale



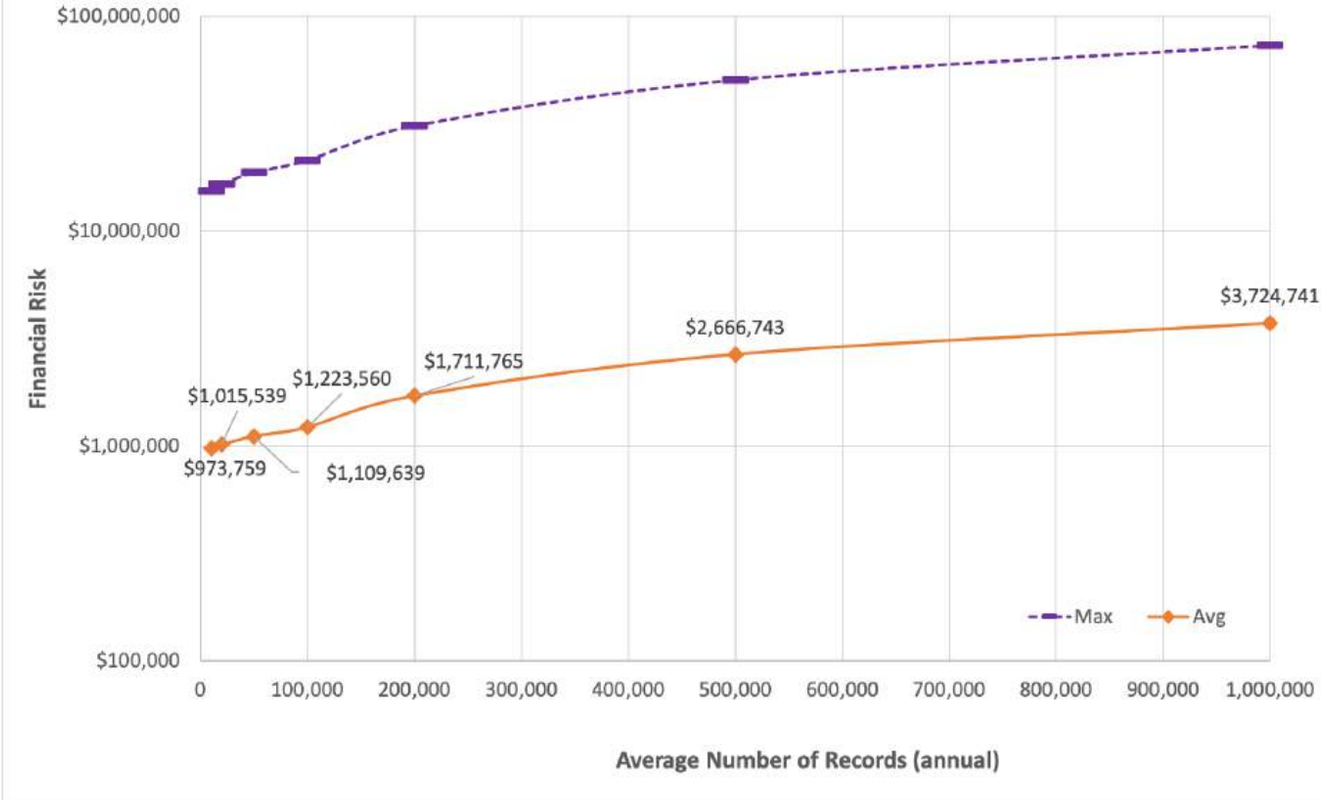
* Financial Risk axis is shown in logarithmic scale

In the Open FAIR terminology, the maximum risk is defined as loss an organization is likely to encounter as a result of a cybersecurity incident.

Third-Party Financial Risk caused by Credit Reporting and Specialty Agencies



* Financial Risk axis is shown in logarithmic scale

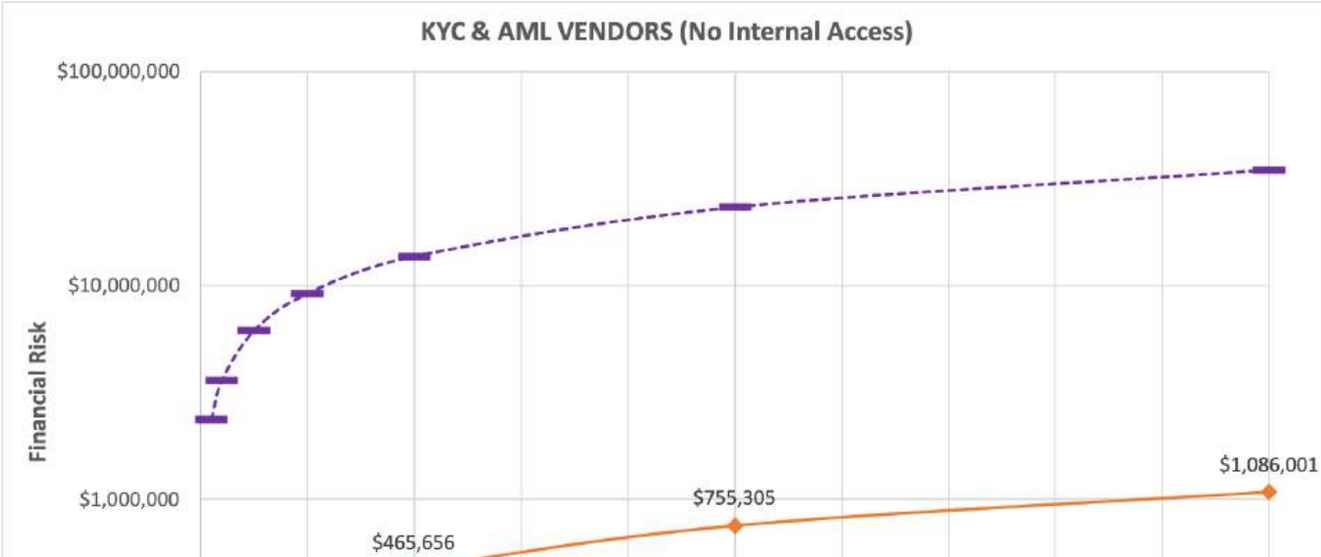


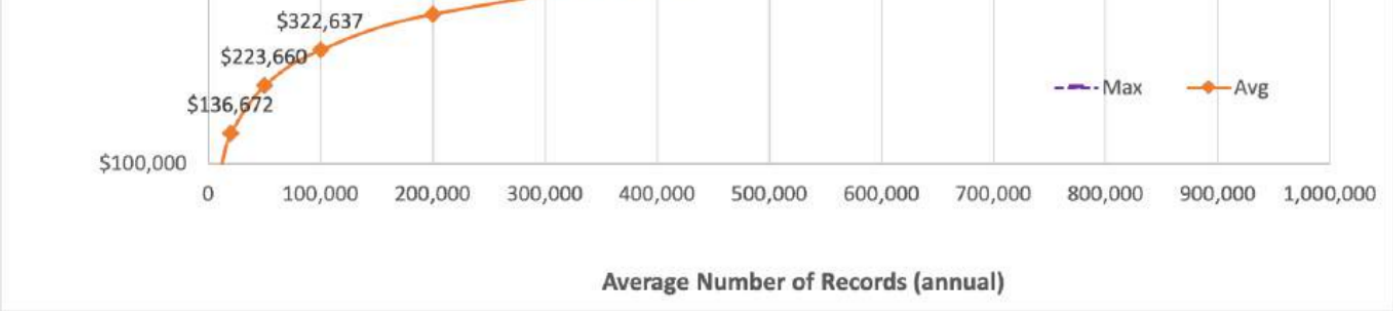
* Financial Risk axis is shown in logarithmic scale

Loss Event Frequency

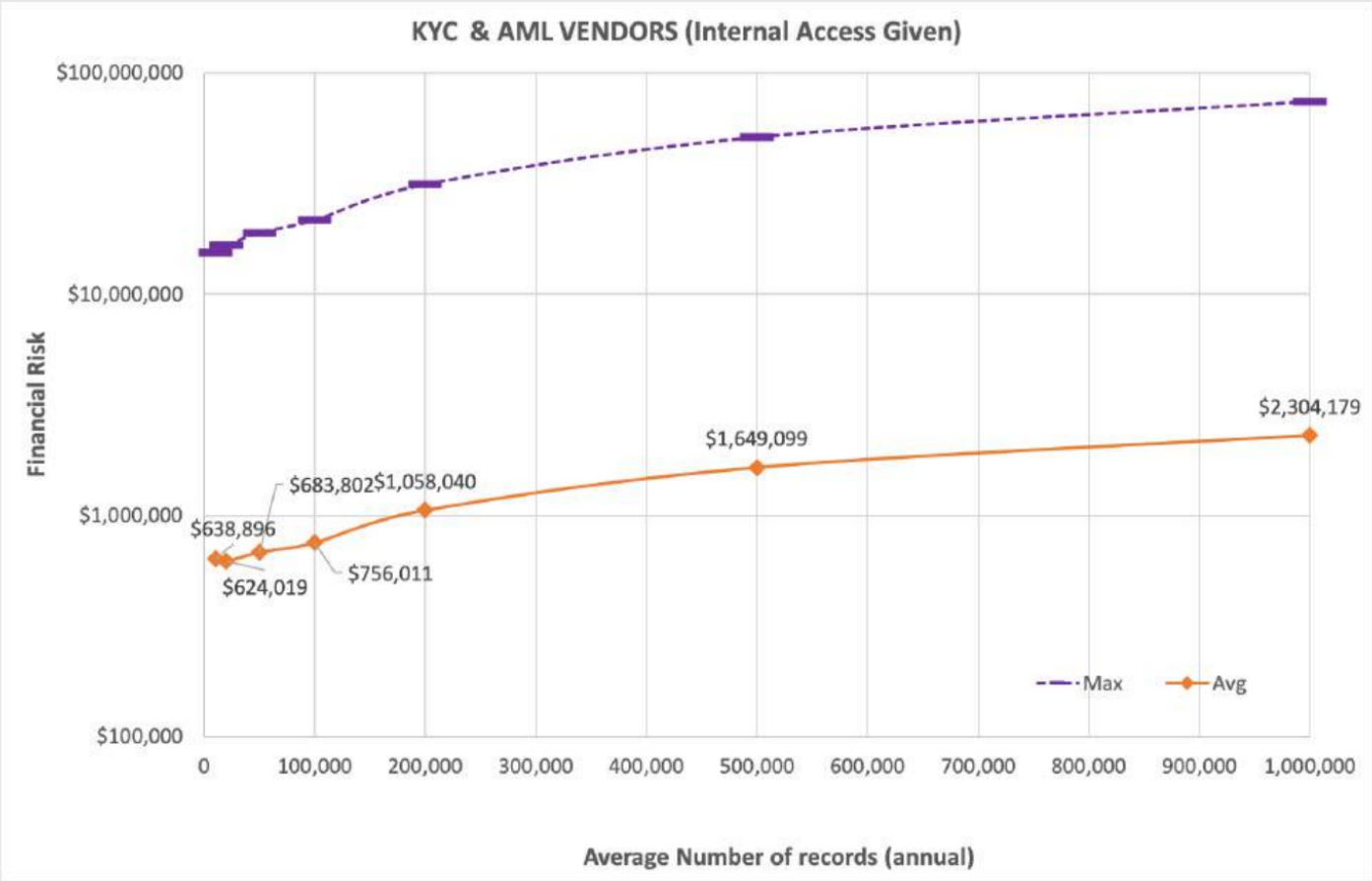
The probable frequency, within a given time-frame, that lost will materialize from a threat agents' action.

Third-Party Financial Risk caused by (KYC)/ (AML)



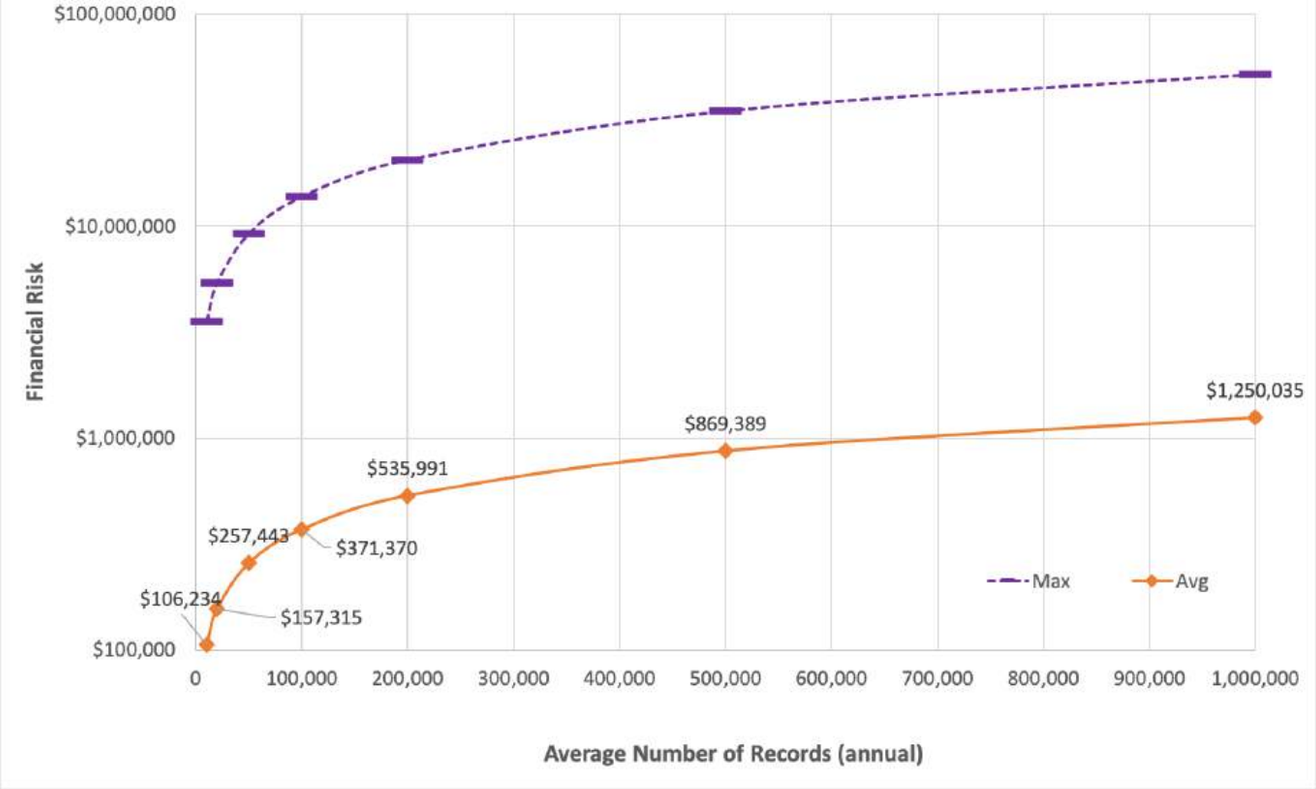


* Financial Risk axis is shown in logarithmic scale

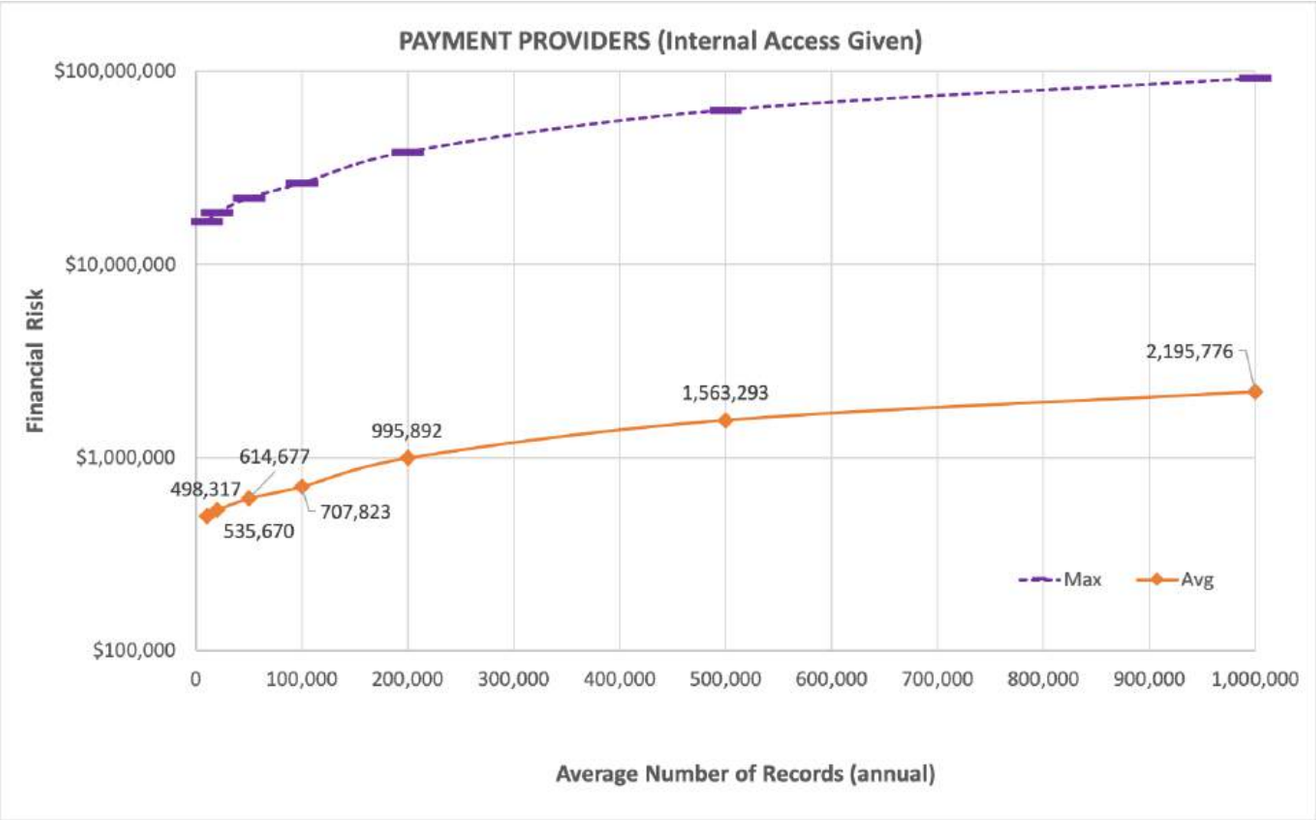


* Financial Risk axis is shown in logarithmic scale

Third-Party Financial Risk caused by Payment Providers



* Financial Risk axis is shown in logarithmic scale



* Financial Risk axis is shown in logarithmic scale

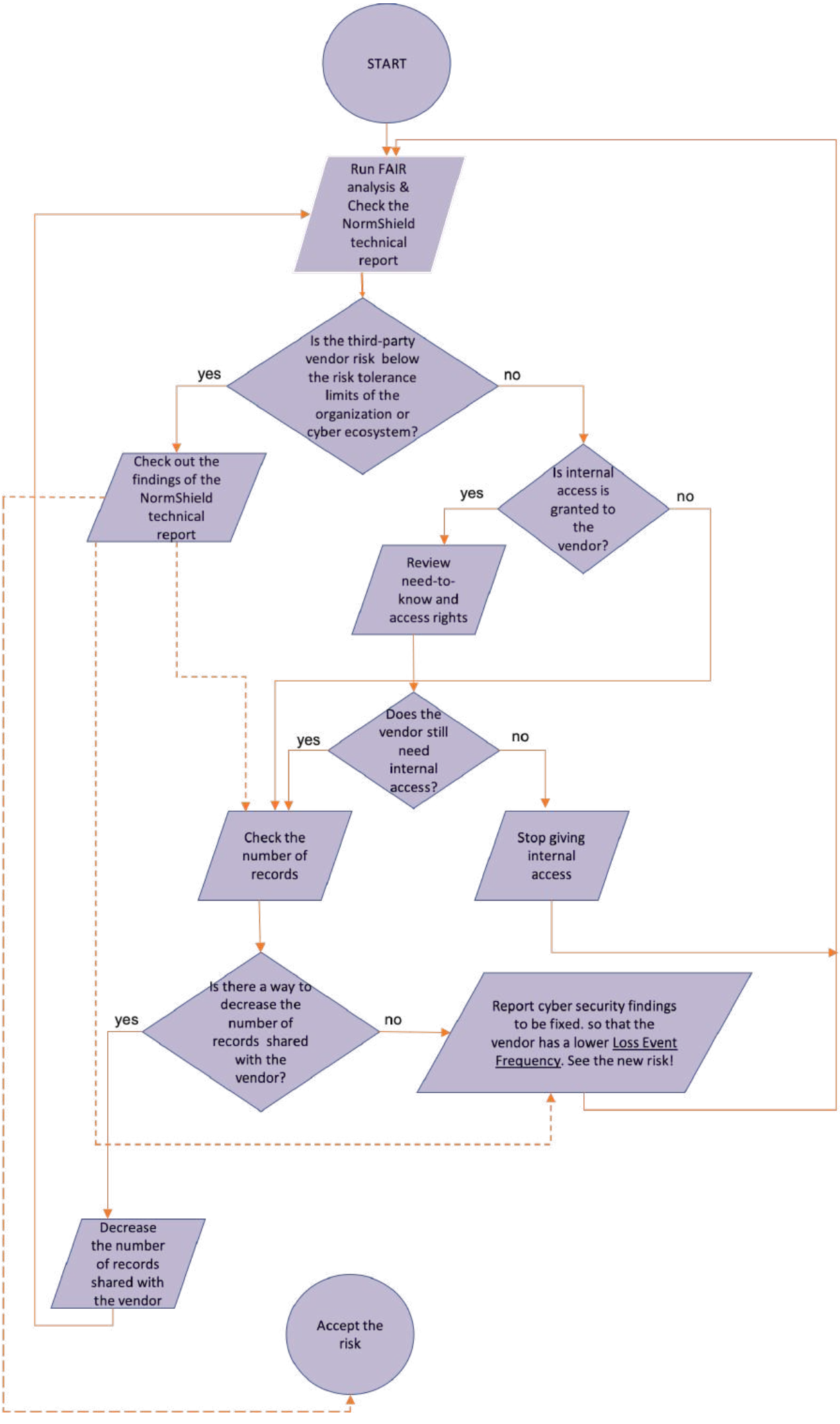
"Ideally, internal access should only be activated on an as-needed basis and disabled when not in use."

What Does the Financial Risk of a Third Party Tell Us?

The Probable Financial Impact Rating NormShield leverages, presents a new language for cybersecurity and risk management professionals. In this new language, the cybersecurity risk is better communicated to upper levels in an organization.

Financial Institutions can make informed decisions on their vendor ecosystem based on the Open FAIR report. Listed in the below section are some of the actions a Financial Institution can take on for third-party risk management.

Third-Party risk


START
Run FAIR analysis & Check the NormShield technical report
Is the third-party vendor risk below the risk tolerance limits of the organization or cyber ecosystem?
yes
no
Check out the findings of the NormShield technical report
Is internal access is granted to the vendor?
yes
no
Review need-to-know and access rights
Does the vendor still need internal access?
yes
no
Check the number of records
Stop giving internal access
Is there a way to decrease the number of records shared with the vendor?
yes
no
Report cyber security findings to be fixed. so that the vendor has a lower Loss Event Frequency. See the new risk!
Decrease the number of records shared with the vendor
Accept the risk