RISK ASSESMENT REPORT

Qwant

The search engine that values you as a user, not as a product

---

Ojie Okodogbe
University of Maryland, College Park
INST464: Decision Making for Cybersecurity
Professor Joe Kelly
May 16 2025

01 ABOUT

02 EXECUTIVE SUMMARY

03 COMPANY OVERVIEW

04 QUALITATIVE RISK ANALYSIS

05 QUANTITATIVE RISK ANALYSIS

06 RECOMMENDATIONS

07 APPENDICES

ABOUT THIS DOCUMENT

Project Description

This report describes the cybersecurity assessment of Qwant, a privacy-focused search engine based in Paris, France. It differs from mainstream search engines in that it provides relevant search results while avoiding data monetization and maintains user privacy. Revenue is generated through non-intrusive methods: contextual advertising and commission-based revenue.

Key Terms

- Computer Security: A system operating in a state where it does what it is supposed to do and only what it is supposed to do.
- Information Security: Information being protected from unauthorized access or alteration while being readily available to authorized individuals when required
- CIA: Confidentiality, Integrity, and Availability—The goal of computer security
- Endpoints: Devices used every day. (Desktops, laptops)
- Personal Data: The GDPR in article 4, defines personal data as follows:
  > "Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
- PII: Personally Identifiable Information
- SPD: Sensitive Personal Data

Limitations

This cybersecurity analysis is based upon external online assessment of the Qwant system. No discussions with any personnel at Qwant occurred, hence, a direct observation of the company's hardware configuration and the day-to-day behavior of staff was not possible. Therefore, this assessment may be missing vulnerabilities and risks related to hardware configuration and user behavior that is not in compliance with best security practice. Some financial values were calculated in United States Dollar and then converted to Euri using 1 USD = 0.92 EUR

Analytical Confidence

I assess the analytical confidence of this project as: Medium.

This business has well defined assets and a few obvious risks that can be quantified and evaluated for the considered set of loss scenarios. Confidence in the probability of loss is therefore medium. As noted above in the limitations section, there is far less confidence in the magnitude of loss due to this being an external online assessment. Because the business financial numbers may be inaccurate, some estimates of losses may be arbitrary. There is low confidence in the amounts of potential loses. Combined these two confidence levels result in an overall confidence between Medium and Low.

EXECUTIVE SUMMARY

This report presents a comprehensive quantitative risk analysis for Qwant, a privacy-focused search engine, focused on two core areas of risk: Loss of System Availability (Server Loss) and Loss of Information Security (Personal Data Breach). The analysis integrates empirical data, financial impact modeling, and open-source intelligence from Qwant's digital footprint, including sources such as LinkedIn, Crunchbase, Yahoo Finance, and Better Web by Qwant. The analysis evaluates threat event frequencies, susceptibility, potential financial impacts, and the effectiveness of proposed mitigation strategies.

The first risk, loss of system availability, is primarily associated with threats such as floods, Distributed Denial-of-Service (DoS) attacks, and internal system failures. With an estimated threat frequency of 0.96 events per year and a susceptibility ranging from 10% to 40%, this risk poses a significant threat to Qwant's operations. If realized, the total maximum financial impact is projected at €1.32 million in the worst-case scenario, with a most likely cost around €229,670. A key mitigation strategy—server decentralization—can reduce the likelihood of loss by eliminating single points of failure, lowering flood susceptibility, and improving overall system resilience. Post-mitigation, the likelihood of loss decreases from 64.1% to 55.7%.

The second risk, loss of information security, involves threats such as credential theft, phishing, insider threats, ransomware, and endpoint compromise. The annual threat frequency is high, reaching up to 40.9 events per year, due to the concentration of privileged users in a relatively small workforce. Susceptibility ranges from 25% to 52%, with primary and secondary financial impacts including productivity loss, legal costs, fines, and reputational damage. The total projected maximum financial impact is €8.19 million, with a most likely scenario around €1.38 million. Proposed mitigations—such as mandating encryption at rest, enhancing credential protection, enforcing VPN use, and applying the principle of least privilege—are expected to reduce susceptibility to between 14% and 36%, significantly lowering the risk profile.

In conclusion, Qwant is advised to prioritize server decentralization, full encryption of personal and sensitive data, comprehensive phishing and access control policies, and a diversification away from Microsoft reliance. These measures will enhance the company's operational resilience and protect its reputation as a privacy-focused, independent search engine.

COMPANY
OVERVIEW

Qwant is a privately held technology company headquartered in Paris, France, with additional offices in Nice and Rouen. Founded on May 1, 2011, by Eric Leandri, Jean-Claude Ghinozzi, Jean-Manuel Rozan, and Patrick Constant, Qwant operates as a European alternative to mainstream search engines, prioritizing user privacy and data protection. With a workforce of approximately 127 employees and an estimated annual revenue of around €17.48 million, Qwant competes with major players like Google and Bing in the digital search market. The company falls under the European Union (EU) regulatory environment and aligns itself closely with GDPR compliance standards.

Business

Qwant generates revenue through non-intrusive advertising where data monetization is avoided, and user privacy is maintained.

Contextual advertising is employed: a model where ads are not based on tracked users' behavior or browsing history, but on search queries. For example, if a user searches "Paris Hotels", travel related ads will populate. It's not specific to the user, but to the context.

Qwant's second revenue stream is commission-based revenue. A fee is earned when users click affiliate links to its partners. This includes partners that integrate services into the search engine like DeepL, TripAdvisor, and PageJaunes.

Some of these partners include:

- Mozilla: They integrated Qwant into custom Firefox versions (desktop and mobile), increasing user access, search volume, and hence ad revenue. Qwant is also a default search option. Mozilla is also a privacy-focused firm, so this partnership strengthens Qwant's brand.
- Affliz: Enhances ad relevance by analyzing search queries, improving click through rates and advertiser return on investment.
- Microsoft: Microsoft is Qwant's biggest partner. Qwant outsources its advertising to Microsoft Advertising and utilizes Microsoft Azure for computing resources and storage to improve services.

Strategic Outlook

Qwant recently partnered with Ecosia in 2024, another European search engine and is focused on European sovereignty and reducing reliance on US big tech. While no major cybersecurity incidents have been reported, the company is aware of its reliance on third-party infrastructure and is actively pursuing more autonomous indexing solutions. Future focus on enhancing search capabilities, reducing external dependencies, and expanding its privacy-focused user base.

Website: (https://www.qwant.com)
Industry: Technology (Sub-industries: Cybersecurity, Privacy, AI)
Digital Footprint: 71% of web traffic from France
Social media: Active on LinkedIn

QUALITATIVE ANALYSIS

Qwant uses computers and information to generate revenue, but if they are not secure, not only could Qwant see a halt in revenue generation, but also a loss of revenue.

Assets

Servers

Qwant has over 400 servers in a data center located in the suburbs of Paris. They are used for several purposes: the front (what we see), crawl (the discovery and updating of content), the storage of texts and images, indexing, mapping, news, Qwant's internal tools and many others. Almost two-thirds of the data center is reserved for the proper functioning of Qwant Search. This is critical for the security of other assets. Qwant's server infrastructure is likely a mix of Windows and Linux operating systems, and most likely Linux heavy.

Internal Software

Internal system and application software manages all the assets and systems in mission-critical systems (IT, Financial, and HR). The IT system uses various software to manage servers, endpoints, network infrastructure and more. The system also contains, processes and manages employee PII and possibly end-user PII. The HR systems will store and process employee personal data. Financial systems will store sensitive financial and employment information, process payroll operations and vendor transactions. Internal software is used to manage access controls that dictate access to these systems, so the security of internal software is crucial for cybersecurity.

Search Engine Service

Qwant's search engine services, Qwant Search and Qwant Junior. Web applications that allow users to query Qwant's search infrastructure and interact with Qwant's backend (algorithms, databases) to retrieve results. This is the company's main operation.

Personal Data

If a user creates an account with Qwant, personal data including name, email address, and IP address, device data, search queries, and various cookies are collected. With user consent, personal data is shared with Qwant's partners: Microsoft, and Batch. This asset also includes personal of employees at Qwant. Once these partners are in possession of this information, their privacy policy applies and they now govern this data, but if there is malpractice on their end, Qwant could still be held responsible. Even though this data is anonymized, links and inferences can still be made.

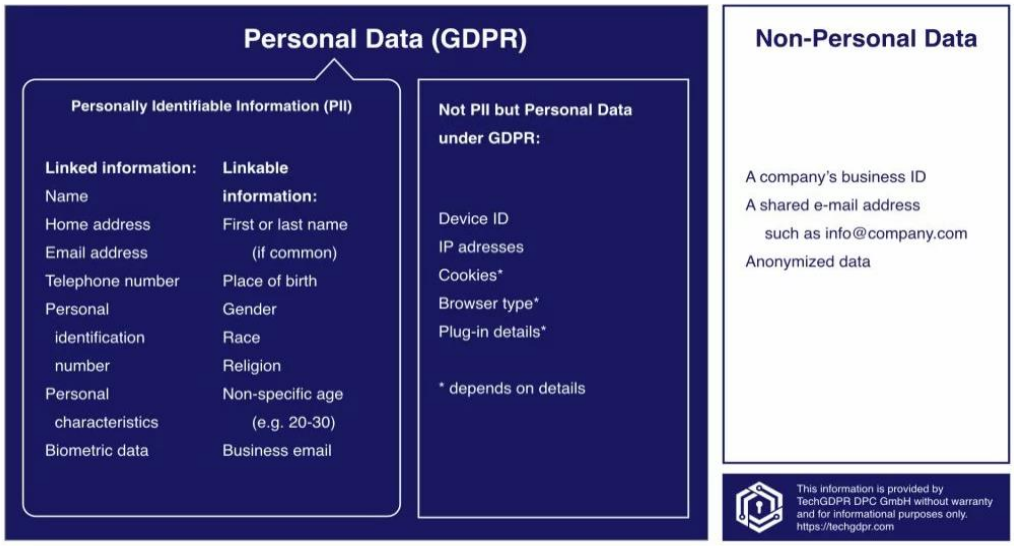


Figure 1

Specifically, Qwant sends anonymized search queries, IP addresses (only first 3 bytes for users without an account) to reveal geographic location and show local ads, and cookies to Microsoft (all considered personal data in EU). But Qwant has multiple mechanisms in place to prevent cross-referencing. To distinguish users for ad delivery without tracking them long term or identifying them, a hash (anonymized ID) based on a user's IP and browser information is created and mixed with a salt (random data that changes every three months). A random identifier is generated for each session. This data pseudonymization tool is critical, without this plain personal data will be shared.

Intellectual Property (IP)

Intellectual Property includes code, algorithms, web indexing technologies, web crawlers, and data anonymization tools that ensure operation and compliance with privacy regulations.

Microsoft Azure Cloud Services

Qwant relies on Microsoft Azure Cloud services for multiple tasks:

- Azure's Kubernetes: To analyze raw data extracted by web crawlers.
- Azure Cloud Storage: To store web pages awaiting indexing. Index more pages and faster, increasing quality of index and web coverage. Increase the size of Qwant's image index and facilitate the learning of models. Store hundreds of millions of images, or several hundred terabytes of images.
- Azure Cloud Computing Resources: To test new indexing methods or new languages. GPU and FPGA-based infrastructures to train "Learning to Rank" models.
- Azure On-Demand Resources: To calculate the graph and the associated scores

Threat Vectors

Physical

A natural disaster near Qwant's data center in Paris (Seine-Saint-Denis or Hauts-de-Seine) can cause physical damage to servers and infrastructure or cause servers to lose functionality. These areas—which are surrounded by the seine river and its tributaries—are flood-prone. This would disrupt Qwant's operations and render the search engine service unavailable. Power outages could occur due to severe weather conditions, also leading to operation disruption.

Denial of Service Attack (DDoS)

A DoS attack on Qwant's servers could disrupt the servers from functioning in their intended state. This might exploit a known vulnerability in a specific server application or operating system. Authorized users are denied access to the system, most likely accomplished by crashing the server and taking it offline or sending so many requests to overwhelm the system. A distributed denial-of-service attack on public-facing services like the authentication portal could be targeted to exhaust CPU resources.

Insiders

As authorized users in an organization that already have access to assets, insiders could exploit weaknesses to launch privilege escalation attacks and gain unauthorized access to certain data & information assets such as PII or other sensitive financial information and systems. With under 250 employees, access controls are most likely not segregated, and privilege accounts might have access to a wide range of critical services. This could also be a disgruntled employee purposely corrupting data and files. Employees could also be targeted with corporate espionage attacks, and if they can gain unauthorized access to personal data and IP this could result in a data breach and loss of operation. Human errors from employees like misconfigured server settings or system and application software could expose assets or create vulnerabilities. Through negligence, employees could become unintentional insider threats by allowing someone to piggyback or shoulder surf them. This could provide attackers with unauthorized access into secure spaces or facilities, and they could proceed with initiating malware attacks. Attackers could steal endpoints like workstations from Qwant's offices, which might contain IP or provide access to the internal network.

Supply Chain

The heavy reliance on Microsoft Azure solutions introduces multiple single points of failure. An outage at Microsoft could lead to a disruption of effective operation and service improvement. As Qwant shares data with its partners Microsoft and Batch, there will most likely be some system integration and this increases the attack surface. If this system integration entails the use of embedded code or automation and a partner is compromised, attackers could transmit malware, and they could be automatically processed. Integration with third-party tools like Cloudflare introduces risk if these vendors are compromised. Once users consent to data sharing with Microsoft, Microsoft's privacy policy now governs the handling of that data. While the data shared is pseudonymized, it can still be linked to individuals when combined with other data. Under the GDPR, pseudonymous data is still considered personal data. GDPR fines could arise from this.

Software Vulnerability
Software vulnerabilities in internal software used to manage assets. Qwant validates input via its sign-up page; if there is a vulnerability in the code, the system could be exposed to cross site scripting (XSS) attacks and SQL injections. Vulnerability in database storing personal data could be exploited.

Credential Abuse
Through a variety of techniques, attackers can gain unauthorized access to employee credentials. Credentials can give attackers access to internal software used to manage assets. This includes PII, IP, and servers. A privilege escalation could be used to elevate permissions, create more accounts or establish an APT. With less than 250 employees, it is likely that some accounts have a high concentration of elevated permissions, rendering spear phishing attempts likely.

Zero Day Vulnerabilities
Zero-day vulnerabilities within Qwant's systems.

AI Threats
Qwant uses AI systems for its web indexing. These systems could be targeted with data poisoning attacks. Malicious actors can flood the internet with malicious content or manipulated content to degrade search engine quality. They could inject biases and false information which could lead to some legal issues. AI web crawlers could download malicious files.

Regulatory Compliance
As Qwant operates within the EU, it needs to comply with the GDPR, which requires strong privacy protections, and is subject to oversight by the CNIL (French data protection authority). Other regulations include the Digital Service Act (DSA), AI Act, and the ePrivacy directive. Under the GDPR, after users consent to the use and processing of their personal data by partners, these partners now become data controllers; they define the purposes and methods of using this data, and are responsible for ensuring its confidentiality, and guaranteeing compliance with laws and regulations. If data controllers could have poor mechanisms for safeguarding this data or breach the GDPR, legal risks and fines could arise. For more serious infringements, a GDPR fine is the higher value of up to €20 million or 4% of global annual turnover (€748,000 for Qwant). For less severe infringements, the fine is the higher value of up to 10 million or 2% of global annual turnover (€374,000 for Qwant). A GDPR violation would warrant €748,000 or €374,000, depending on the violation.

Threat Actors

The most likely actors to target Qwant include:

- Nation-state actors
    - Motivation: Political and Strategic
    - Detail: Nation states with an interest in preventing Europe from developing an independent search engine. Independent of U.S-dominated search engines. Might include Russia, China and the U.S.
- Hacktivists: Ideology
    - Motivation: Ideological and Political
    - Detail: Parties that might not agree with Qwant's practices. May disagree with Qwant's privacy claims. Might dislike Qwant's partnership with a big U.S tech firm like Microsoft.
- Insiders:
    - Motivation: Financial, Negligence, Dissatisfaction, Human error.
    - Detail: Disgruntled employees or employees in disagreement with some practices might leak information or trade secrets. Human error.
- Cybercriminals:
    - Motivation: Financial
    - Detail: Seeking financial gain. Might be looking to gain unauthorized access to information assets. Could launch a ransomware attack or sell to third parties.
- Competitors:
    - Motivation: Economic, Strategic
    - Detail: Competing firms. Could be non-privacy focused search engines worried about losing users. Could orchestrate a data breach to damage Qwant's reputation. Will most likely launch attacks through proxies.
- Regulatory bodies:
    - Bodies: National Communication on Information and Liberty (CNIL), National Cybersecurity Agency of France (ANNSI), European Commission.
    - Will issue fines for breaching legislation.
- Script Kiddies:
    - Motivation: Financial, Attention, Fun, Curiosity
    - Detail: Might want to find any vulnerabilities and exploit it. Attacks are easier to launch with the prevalence of large language models (LLM's).

Risk Scenario Matrix

Asset	Threat Methods	Threat Actors	Loss Types	Scale
Servers	• DoS • Software Vulnerability • Misconfiguration • Stolen Credentials • Natural disasters • Zero Day	• Hacktivists • Cybercriminals • Nation States • Insiders • Competitors • Script Kiddies	• Loss of Revenue • Response Cost • Repair Cost • Reputation	High
Personal Data	• Phishing • Stolen Credentials • Vulnerability Exploit • Privilege Misuse	• Cybercriminals • Competitors • Insiders	• GDPR fines • Cost of legal fees	High
Search Engine Service	• Web Application Attacks • Data Poisoning • DoS	• Hacktivists • Nation States • Insiders • Competitors • Script Kiddies	• Cost of lawsuits • Customer Distrust • Boycotting	High

Figure 2

Risk Scenario Summaries

Loss 1: Loss of System Availability - Server Loss

Server is lost temporarily or permanently. If the attack is strong enough, it could take out all servers because they're in one location. This is a loss event that doesn't involve an attacker getting into Qwant's system. Low chance of occurrence, but high impact.

Asset

Physical Servers. 400 servers located at Qwant's data center. Almost ⅔ of the data center is reserved for the proper functioning of Qwant search. If this is lost, Qwant can't make money.

Threats

Physical threats, natural disasters (will have an impact because 400 servers are all in the same location) and a DoS attack.

Threat Vectors

- Floods, internal and system failure. As Qwant is in the Paris region, flood is the most likely natural disaster but cases of data centers being affected by flooding have not been reported in the Paris region. If Qwant has good physical mechanisms in place, Qwant will most likely be fine.
- DoS attacks to overwhelm Qwant's resources. It will probably render some functionality unavailable but not all. But Qwant has Cloudflare, so this is unlikely. Unless there are misconfigurations or software vulnerabilities.

Threat Actors

- Natural event of flood.
- DoS attacks will most likely be launched by hacktivists, competitors and nation-state actors. There is no financial gain so it is unlikely that it will be cybercriminals, script kiddies wouldn't have the resources. Something like this would be more ideological, economic or political.

Losses

- Search engine service is down so Qwant can't generate revenue from ads, or from Qwant's partners. No revenue at all.
- For physical, if all servers are lost, Qwant will be out for an extended period. Costs to respond. Costs to repair and replace. Can be expensive if both server equipment, infrastructure and buildings are damaged. Purchase new servers, new equipment and work towards a new data center.
- Qwant might face lawsuits/legal fees if there are any injuries or loss of life to data center workers, GDPR fines are only likely only if stored personal data is lost and Qwant had poor security/protection mechanisms in place.
- A DoS attack will have less impact. Qwant will be down, but it will be temporary. So, no revenue but only for a certain amount of time.

- Most likely loss of revenue for a few days, response cost, investigation cost, repair cost if any crashes or system failures occur, slight reputational damage, shouldn't face any legal fees or lawsuits from this. Biggest risk comes from permanent server loss.

Loss Scenario 2: Loss of Information Security - Loss of Personal Data

In this loss scenario, an attacker gaining access to personal data means a loss of confidentiality. Because they have access, this means they can alter this information, which means a loss of integrity. If there are no backups of this personal data, and an attacker steals it, this means a loss of availability.

Multiple departments at Qwant—including IT, HR, and Finance—will possess a high concentration of internal personal data (personal data of staff), and this increases the attack surface. Individuals in these departments that have access to databases and systems containing personal data can be recruited by malicious actors or targeted with phishing or spear phishing to gain their credentials. Non-department specific, all staff will have access to organizational charts and information databases, which contain personal data. They can also be recruited or be targeted with phishing or spear phishing attacks and password attacks. It is important that strong passwords are enforced to reduce the risk of various password attacks—including password guessing, brute force, dictionary, spraying, hybrid attack (dictionary and brute force). Successful gaining of credentials can allow privilege escalation, lateral movement, and allow the attacker to remain undetected and establish an APT or create backdoors. It is important for each department to have robust information security measures. Unless an internal error is made, this is a loss scenario that requires system intrusion.

Asset

Internal Personal Data (Personal Data of Employees)

Threat Vectors

- Credential Theft: The accounts of individuals that have access to databases and systems containing personal data can be targeted with various password attacks—including password guessing, brute force, dictionary, spraying, hybrid attack (dictionary and brute force).
    - Phishing: Individuals that have access to databases and systems containing personal data can be targeted with phishing or spear phishing attacks to gain their credentials.
- Insider Threats: Individuals in these departments that have access to databases and systems containing personal data can be recruited by malicious actors. Especially individuals in critical departments—like IT—because they have lateral movement, can alter access controls, cover their tracks, and can gain access to personal data contained in other departments.
- Ransomware: Financial malicious actors can collect personal data and render this unavailable to us unless Qwant pays a fee.
- Endpoints: Endpoints could contain personal data. This will require system intrusion (most likely one of the techniques listed above) unless the attacker has physical access to the

endpoint. In this case, if personal data is stored locally, the attacker could use techniques to gain access to it if the drive is not encrypted.

Threat Actors

- Insiders: Disgruntled employees or employees recruited by malicious actors
- Hackers: Financially motivated
- Hacktivist: Ideologically motivated. Hackers might target a privacy focused firm.

Losses

Because Qwant is a privacy-focused firm, this will have severe impacts.

- It will reduce confidence in Qwant's current users and deter new users, which means less revenue as there will be less users to view ads.
- Reduction in non-intrusive advertising revenue and commission-based revenue could lead to a loss of partners.
- As a leading European search engine, this will strengthen the notion Europe cannot be independent and survive without U.S-dominated search engines.
- It will reduce Qwant's potential for future business opportunities. It might deter other firms considering partnering with us from doing so. It could also reduce the confidence of Qwant's current partners.
- Could reduce the confidence of Qwant's internal employees. Working for Qwant, these are most likely privacy-focused individuals. They will be unhappy with a loss of confidentiality of their personal data. Qwant could see employees quitting their jobs and lawsuits arising.
- Lastly, Qwant will have GDPR fines.

Heat Map of Risk Scenarios

A visual representation plotting Probability of Loss Event vs. Severity of Impact.

Certain >90%				
Very Likely 65%-90%				
Likely 35%-65%				
Unlikely 10%-35%			**Loss of Personal Data**	**Loss of Server**
Possible <10%			**Data Poisoning Attack**	
Probability vs Severity	Low	Medium	High	Severe

Figure 3

QUANTITATIVE ANALYSIS

Risk Assessment 1: Loss of System Availability - Server Loss

Asset: Servers
Threat Methods: Flood, Internal System Failure, DoS
Threat Actors: Natural Events, Hacktivist, Nation-State Actor, Competitor
Loss Types: Loss of Revenue, Response Cost, Server Repair Cost, Legal Fees from injuries or loss of life/ Investigation Cost, Reputational Damage, GDPR Fines

Threat Event Frequency (TEF)

Flood: 0.16 per year

- 4 floods in the 21st century (past 25 years) in the Paris region so 4/25 returns a TEF of 0.16 per year.
- DoS Attacks: 0.7 per year
    - This is split into DoS by threat actors: Hacktivist, Nation-State Actor and Competitor. Sum TEF values for each actor returns 0.7 per year.
    - Hacktivist will not have unlimited resources to launch DoS attacks so TEF will probably be around 0.4 per year.
    - Nation-State is very unlikely but unpredictable geopolitical shifts render TEF for this at 0.2 per year.
    - Competitor is unlikely as it's unethical and there have been no reported cases but still possible. TEF for this will probably be around 0.1 per year.
- Internal System Failure: 0.1 per year
    - With around 400 servers, minor failures can be expected but system failure that can result in server loss is much lower at 0.1 per year. 0.08-2 per year.

Susceptibility: 10%-40%

- Flood: 8%
    - Not likely. Floods in Paris have no reported cases of affecting data centers. suggests if a company has good physical protection, there is low risk. 5%-10%.
- DoS: 3%
    - Cloudflare 2023-2024 data suggests no bypasses for systems adhering to best practices. Also reports majority of DDoS attacks end under 10 minutes, only 11% last over 24 hours. Only issues would be misconfiguration, human error or zero day. 2-5%.
- Internal System Failure: 20%
    - Susceptible to frequent minor issues but not issues that should cause server loss. Lower chance as no reported cases of server loss from system failures have been reported. Report found only 10% of publicly reported outages in 2023 were secure.

Qwant likely has a good infrastructure, but server centralization makes this a little higher. HVAC could take all servers out. 10%-20%.

Primary Loss Magnitude:

- Productivity Loss: $51,200 per day
    - Annual revenue is estimated at 18.7m per year. Daily, this is around $51,200 per day. $30,720 - $81,920

- Response Cost: $11,900
    - Staff Overtime: 7 Staff * $50 *24 hours = $8400
    - External Consulting = Average cost of $2500
    - Combined returns $11,900
    - $8400-$20,000

- Replacement Cost: $750,000
    - Most likely servers are Lenovo ThinkSystem SR650(most used hardware in France, costs $2250) and Dell Power Edge R740(most used in the world, costs $4000). Assume a 50/50 split of both servers: 200 dell, 200 Lenovo
    - Replacement Cost= 200 Lenovo servers * $2250 + 200 dell servers * $4000.
    - Returns $1.25 million (max). Most likely = $750,000. Min = $62,000

Primary Loss Magnitude			
Loss Type	Min	Most Likely	Max
Productivity	€28,262	€47,104	€75,366
Response	€7,728	€10,948	€18,400
Replacement	€57,040	€690,000	€1,150,000

Secondary Loss Event Frequency: 5% - 40%

- Server loss is likely to lose personal data stored on servers, but GDPR fines will only arise if poor security mechanisms were in place. Qwant has good information security mechanisms, and given that this is a natural event, it is unlikely that this will trigger a GDPR fine.
- A flood affecting the data center might lead to injuries or loss of life which might incur legal fees, but this is unlikely—no similar cases have been reported.
- Internal system failure or DoS attack will do reputational damage. But DoS is very unlikely to happen. 5%-40% estimated. 35% Most likely.

Secondary Loss Event Frequency		
Min	Most Likely	Max
5%	35%	40%

Secondary Loss Magnitude:

- Response Cost: $1- $10,000
    - Greater amount to legal fees. Most likely around $4800. Avg. legal fees $200 per hour, $200*24=$4800.
- Competitive Advantage Loss: $10,000-$50,000
    - Unlikely to lose partners from this. Probably $20,000.
- Fines: $1-$80,000
    - Most likely $20,000.
- Reputational Damage: $50,000 - $500,000.
    - Loss of information security will result in devastating reputational effects that will be magnified because Qwant is a privacy-focused firm. Could lead to boycotting of the service.
    - Damages the Qwant's reputation as an independent search engine. Might reinforce doubts about if Europe can be independent and survive without U.S-dominated search engines. Can lead to a lack of confidence amongst Europeans.
    - Most likely $100,000.

Secondary Loss Magnitude			
Response	€0	€4,416	€9,200
Competitive Advantage	€9,200	€18,400	€46,000
Fines	€46,000	€230,000	€0
Reputational Damage	€230,000	€460,000	€2,300,000

Pre-Mitigation Loss Exceedance Curve

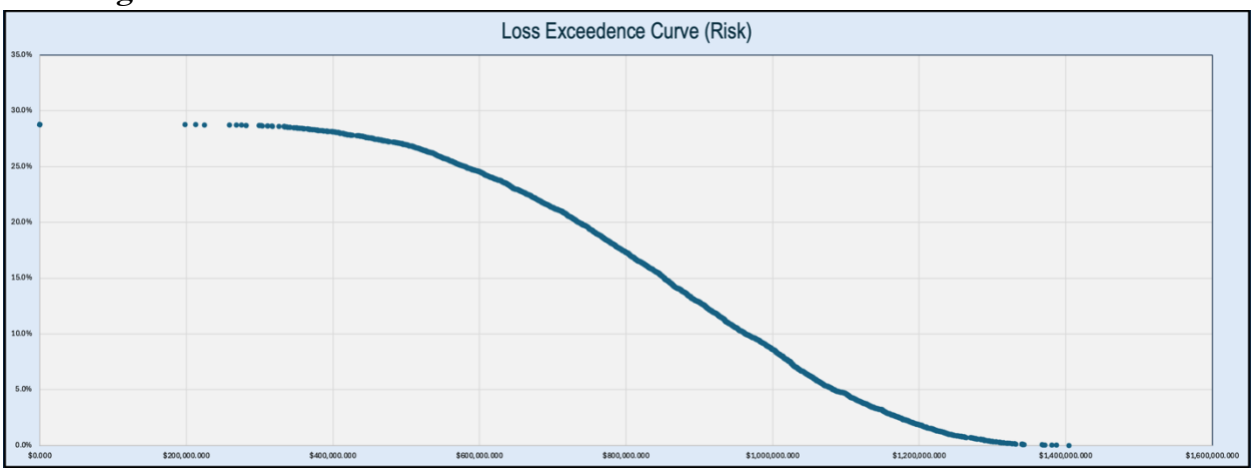


Figure 4

Mitigation

Server Decentralization: Investigate another Data Center away from the Paris region. Reduces impact of flooding and reduces a single point of failure.

- Reduces Flood TEF by half (0.16 to 0.08). Reduces Flood susceptibility by half (8% to 4%). Reduces System Failure TEF from 0.1 to 0.08. Reduces System Failure Susceptibility by half (20% to 10%).
- Reduces TEF to 0.86 and SUSC. to 17%
- Reduces likelihood of loss from 64.1% to 55.7%

Post-Mitigation Loss Exceedance Curve

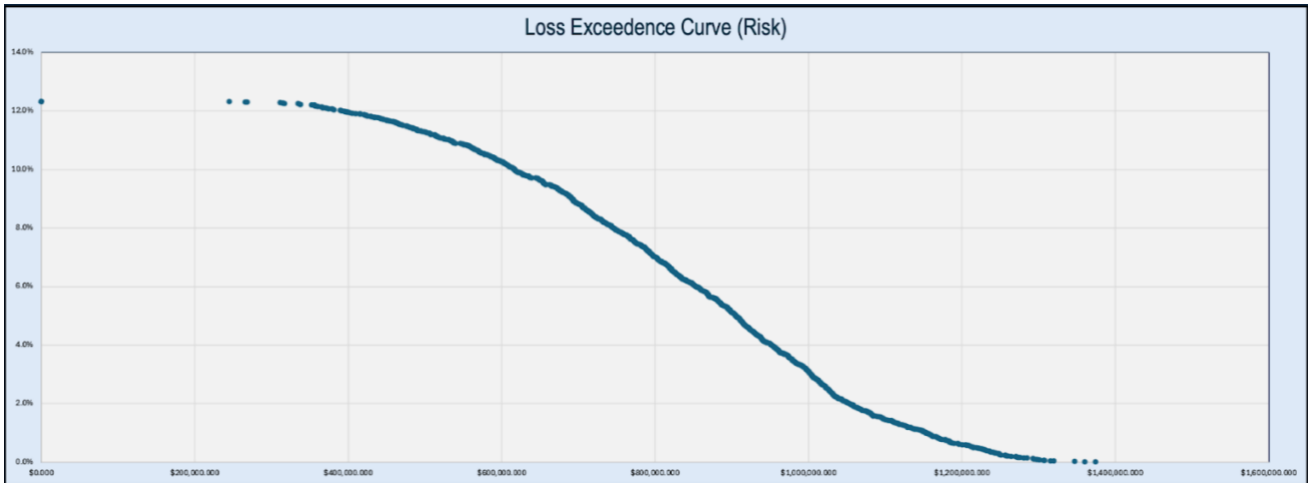


Figure 5

Risk Assessment 2: Loss of Information Security - Loss of Personal Data

Asset: Internal Personal Data
Threat Vectors: Credential Theft, Phishing, Insider Threats, Ransomware, Endpoints
Threat Actors: Hacker, Insider, Hacktivist
Loss Types: Revenue loss, customer loss, loss of possible business opportunities, sever reputational damage, GDPR fines, lawsuits

Threat Event Frequency: 40.9 threat events/year

- Credential Theft: 40 threat events/year
    - Phishing: 30/year
        - 1 phishing attempts/year for high-value employees (IT, Finance, HR)
        - Qwant has 127 employees, so assume:
        - 30 high-value staff × 1 = 30 attempts/year
        - Estimated phishing threat events/year = 30
    - Password Attacks: 10 threat events/year
        - Assume exposed login portals or services (e.g., Outlook Web, internal VPN, dev services).
        - Credible password guessing, Dictionary attacks.
- Insider Threat: 0.3 threat events/year
    - 0.5 malicious insider recruit attempt annually
    - 0.1 malicious activity by insider annually
    - 0.5+0.1/2=0.3
- Ransomware: 0.3 threat events/year
- Endpoints: 0.3 threat events/year
    - Credential theft techniques for system intrusion above apply
    - 0.3 endpoint theft attempts annually

Susceptibility: 25%-52%

Credential theft: 10%-15%

- Low because Qwant has a low number of employees. But high because this means a high concentration of privileges.
- Individuals with a high concentration of privileges in the IT department will most likely have stronger phishing training and education about strong passwords.
- Finance and HR individuals present more risk.
- Around 2%-5% for educated individuals, 10%-15% for lower security educated individuals.

Insider threat: 5%-20%

- Rare and unlikely but impactful. 10%-20%

Ransomware: 5%-10%

- Requires system intrusion and financial exploitation will only be successful if there is no backup. Low risk of financial extortion but there will be loss of confidentiality. 5%-10%.

Endpoints: 3%-7%

- Rare but impactful if the drive is unencrypted and contains personal data. 3%-7%.

	TEF			SUSC.		
	MIN	ML	MAX	MIN	ML	MAX
Credential Theft	1	9	40.9	10%	12%	15%
Insider Threat	0.1	0.3	0.5	5%	9%	20%
Ransomware	0.1	0.3	0.5	5%	7%	10%
Endpoints	0.1	0.3	0.5	3%	5%	7%
	1.3	**5**	**40.9**	**25%**	**43%**	**52%**

Primary Loss Magnitude

- Productivity Loss: €1600-€12,000
    - Estimate 2-15 employees unable to work efficiently for 16 hours (2 workdays)
    - Hourly wage * X hours of work that could not be completed:
        - €50*16*2= €1600 | €50*16*30= €12,000
- Response Cost: €8400-€10,000
    - External Consulting: €2400-€4000
        - Estimate 16 hours of external consulting
        - Average cost * 16 hours:
        - (€150-250/hours) * 16 hours = €2400-€4000
    - Staff Overtime: €6,000
        - 15 critical staff working overtime to investigate, respond and mitigate
        - 15 staff working additional 6 hours for 2 days
        - Hourly wage *15 staff * 4 hours * 2 days
            - €50*4*15*2= €6,000
- Replacement Cost: €0 - €1.5 million
    - Ransomware cost: €0 - €500,000. Most likely €32,000.

Primary Loss			
Loss Type	Min	Most Likely	Max
Productivity	€1600	€5,000	€12,000
Response	€8400	€8500	€10,000
Replacement	0	€32,000	€500,000

Secondary Loss Event Frequency: 58%-83%

- GDPR fine is highly likely. A successful data breach will mean a higher fine. Lawsuits are not very likely.
- Reduction in non-intrusive advertising revenue and reduction in commission-based revenue is highly likely.
- Loss of partner due to a reduction in affiliate link clicks is moderately likely.

Secondary Loss Event Frequency			
Loss Type	Min	Most Likely	Max
GDPR Fine	60%	80%	95%
Lawsuit	40%	50%	70%
Reduction in non-intrusive advertising revenue	80%	90%	95%
Reduction in commission-based revenue	80%	90%	95%
Loss of partner due to affiliate click loss	30%	35%	60%
Average	58%	69%	83%

Secondary Loss Event Frequency		
Min	Most Likely	Max
58%	69%	83%

Secondary Loss Magnitude

- Response Cost: €5,000 - €25,000
  - Legal/Lawyer fees and PR costs: €5,000 - €25,000
- Competitive Advantage Loss: €10,000 - €500,000
  - Loss of partners/delayed growth: €10,000 - 250,000
- Fines: €20,000 - €350,000
  - GDPR fines: €20,000 - €250,000
  - Lawsuits: €0 - 100,000
- Reputational Damage: €30,000 - €600,000
  - Brand damage: €10,000 - €250,000
  - Reduction in non-intrusive advertising revenue: €10,000 - €200,000
  - Reduction in commission-based revenue: €10,000 - €150,000

Pre-Mitigation Loss Exceedance Curve

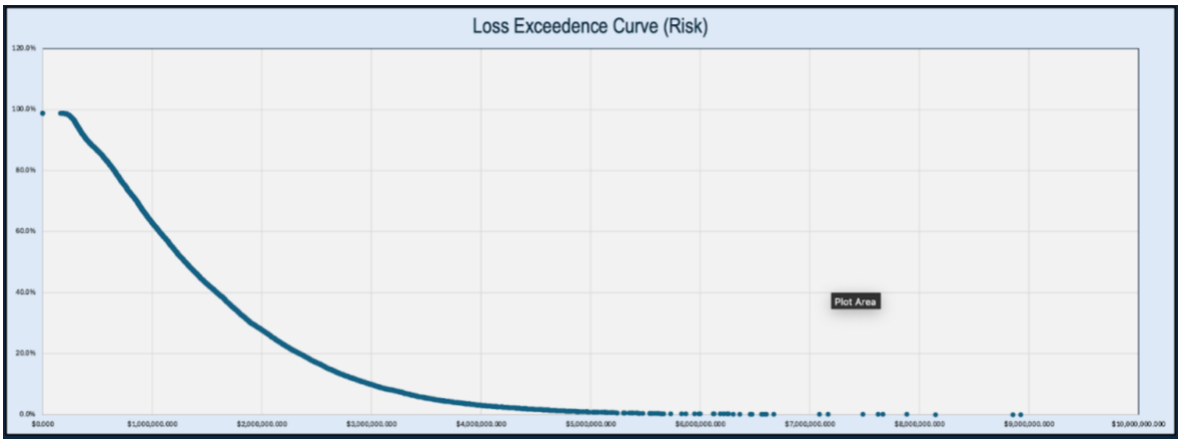


Figure 6

Mitigations

- Encryption at Rest: In case of loss of computer or server security, information security is maintained. BitLocker and File Vault mandating.
- Credential Protection:
    - Effective phishing training
    - Mandating the use of VPN to connect to company resources
    - Principles of least privilege

	TEF			SUSC.		
	MIN	ML	MAX	MIN	ML	MAX
Credential Theft	1	9	40.9	**6%**	**8%**	15%
Insider Threat	0.1	0.3	0.5	**3%**	**5%**	**8%**
Ransomware	0.1	0.3	0.5	**4%**	**5%**	10%
Endpoints	0.1	0.3	0.5	**1%**	**1%**	**2%**
	1.3	**5**	**40.9**	**14%**	**19%**	**36%**

Note: Bold format indicates changes from mitigations.

Impacts:

Reduces Susceptibility values to 14%, 19% and 36%

Reduces Loss event frequency to 0, 2.2, and 10 respectively

Post-Mitigation Loss Exceedance Curve

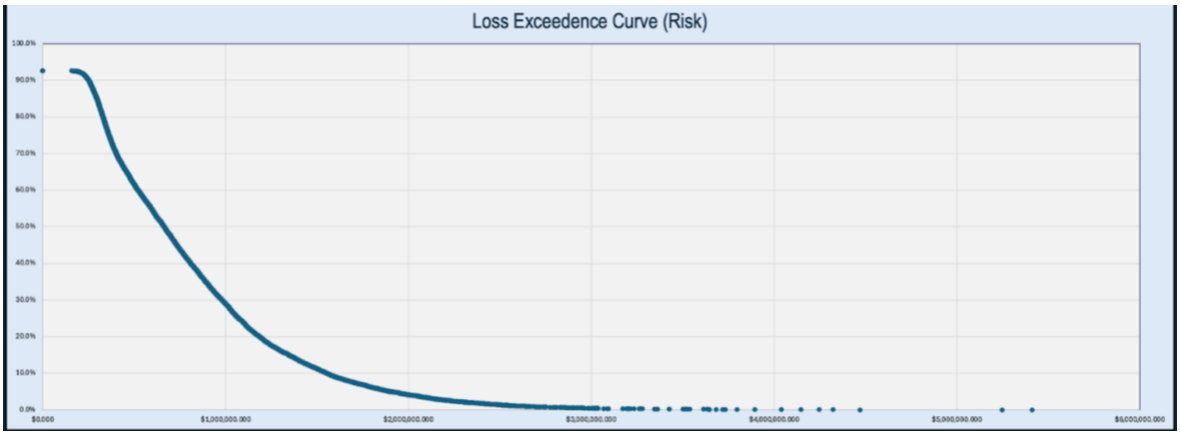


Figure 7

R E C O M M E N D A T I O N S

Server Decentralization: Qwant possesses over 400 servers in one data center. Centralization introduces a single point of failure.
Recommendations:

- Migrate to a geographically distributed server structure
- Ensure redundancy for servers that power the proper functioning of Qwant search because this is vital for revenue generation. In the case of any disaster, Qwant can still generate revenue.

Encryption at Rest: In case of loss of computer or server security, information security is maintained.
Recommendations:

- Enforce encryption of all personal data of employees and any sensitive information.
- Mandate BitLocker for Windows and File Vault for Apple on all endpoints.

Credential Protection: Qwant is small which means there will be a high concentration of privileges for certain individuals. It is important that the credentials of these individuals are highly protected. Unauthorized access could allow the attacker to have lateral movement and create backdoors.
Recommendations:

- Effective phishing training.
- Mandating the use of VPN to connect to company resources.
- Principles of least privilege.

Reduce Microsoft Reliance: Reduce heavy reliance on Microsoft to reduce multiple single points of failure.
Recommendations:

- Explore other backup storage options.
- Explore other backup computing resources as a backup.

A P P E N D I C E S

Spreadsheet of FAIR Model Results

Risk Scenario 1: Loss of System Availability - Server Loss

Pre-Mitigation FAIR Model Spreadsheet

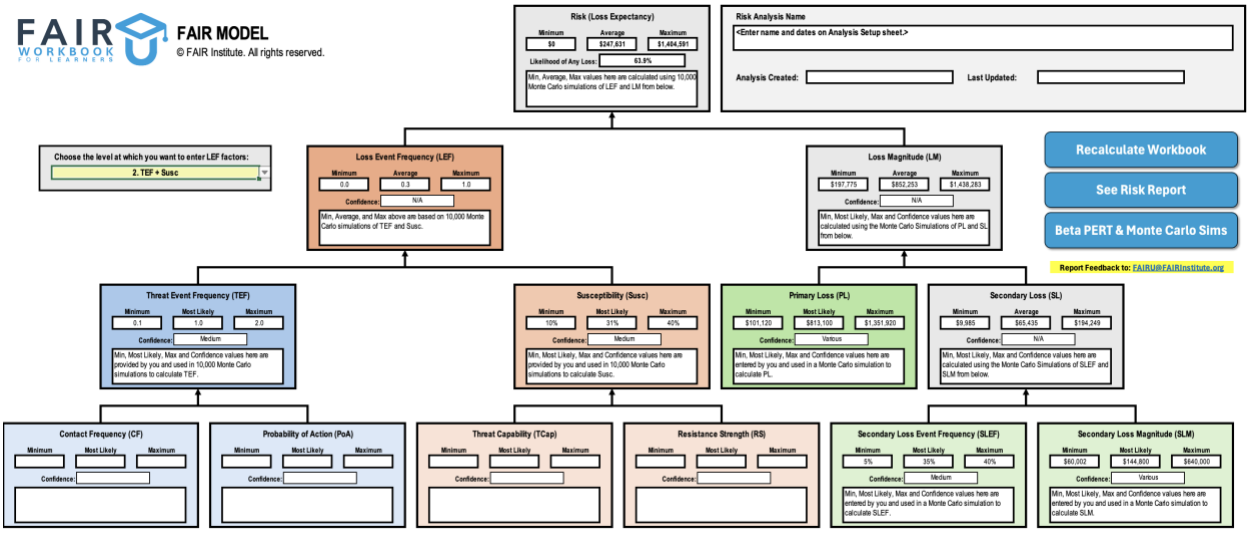


Figure 8

Post-Mitigation FAIR Model Spreadsheet

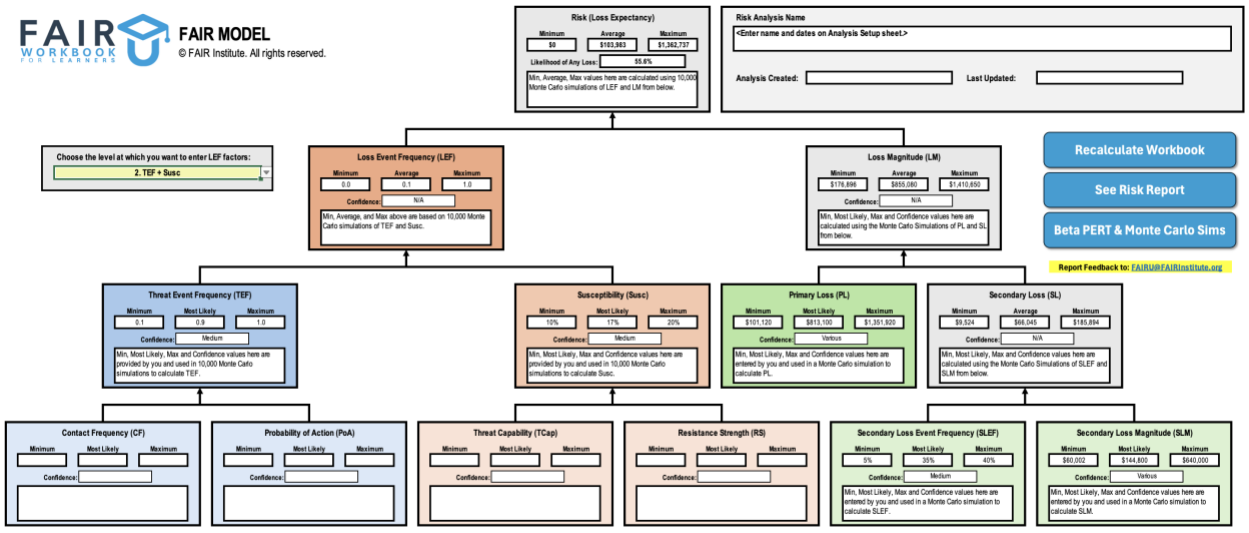
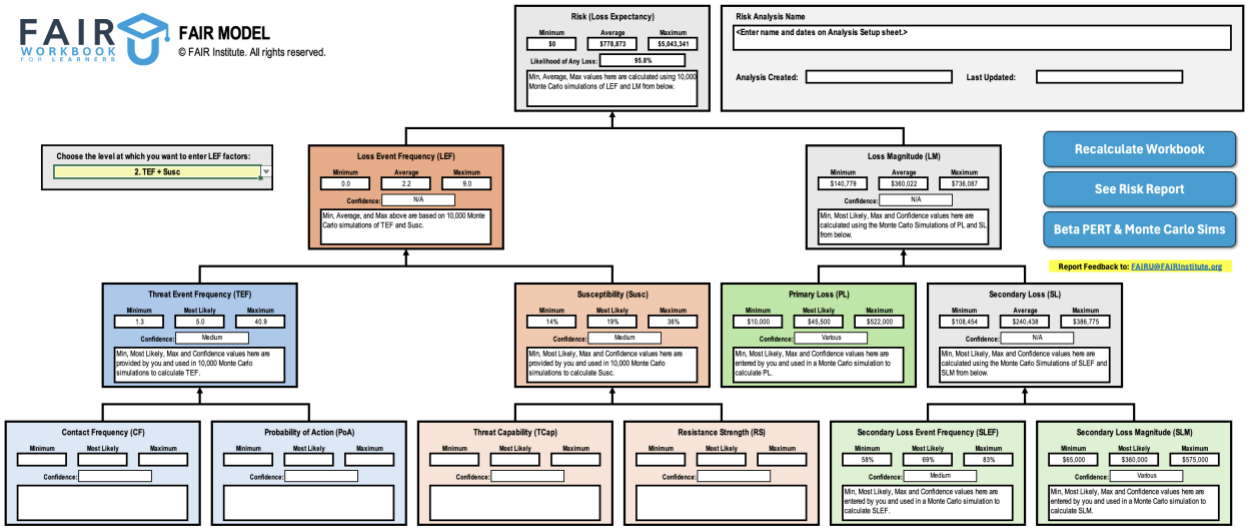


Figure 9

Risk Scenario 2: Loss of Information Security - Loss of Personal Data

Post-Mitigation FAIR Model Spreadsheet



References

1. Qwant. (n.d.). LinkedIn. https://www.linkedin.com/company/qwant/
2. Qwant. (n.d.). Crunchbase. https://www.crunchbase.com/organization/qwant
3. Qwant. (n.d.). Rocket Reach. https://rocketreach.co/qwant-profile_b5e8c0d4f42e7e15
4. Qwant. (n.d.). Yahoo Finance. https://finance.yahoo.com/quote/qwant/
5. Qwant. (2023, September 18). Web indexing: Where is Qwant's independence? Better Web by Qwant. https://betterweb.qwant.com/en/2023/09/18/web-indexing-where-is-qwants-independence/
6. Qwant. (n.d.). Privacy policy – non-consent. Qwant Legal. https://about.qwant.com/en/legal/confidentialite/#non-consent
7. Qwant. (2019, June 25). How Microsoft tools strengthen Qwant. Better Web by Qwant. https://betterweb.qwant.com/en/2019/06/25/how-microsoft-tools-strengthen-qwant/
8. Digital Policy Alert. (n.d.). CNIL issued compliance reminder in investigation into Qwant over alleged wrongful privacy policy. https://digitalpolicyalert.org/event/26966-cnil-issued-compliance-reminder-in-investigation-into-qwant-over-alleged-wrongful-privacy-policy
9. Tech GDPR. (n.d.). Difference between PII and personal data. https://techgdpr.com/blog/difference-between-pii-and-personal-data/