Assessment of Financial Risks Arising from Cybersecurity Threats in a Small IT Company

Batuhan Ketene

2025 Laurea

Laurea University of Applied Sciences

Assessment of Financial Risks Arising from Cybersecurity Threats in a Small IT Company

Batuhan Ketene

Safety, Security & Risk Management

Thesis

12,2025

Laurea University of Applied Sciences **Abstract**
Safety, Security and Risk Management
Bachelor

Batuhan Ketene
Assessment of Financial Risks Arising from Cybersecurity Threats in a Small IT Company
Year 2025 Number of pages 47

The objective of this thesis is to identify, analyze and mitigate financial risks that are caused by cybersecurity threats in small information technology company. By developing a practical and lightweight approach, this thesis aims to better understand the cause and effect relation between financial risks and cyber threats using Company X as a case company. The knowledge base derives from risk management guidelines and operational realities of small IT businesses. This thesis applies qualitative and developmental methods such as a document analysis, a targeted literature search to build the theoretical framework, a semi structured interview with the Company X, a brainstorming session, and a SWOT analysis.

The first step was to do a risk assessment that focused on cybersecurity to identify and look at threats that could cause financial instability in a small SaaS company. Identified risk were evaluated using a simple scoring model that uses likelihood and impact parameter and summarized the risks in a prioritization matrix. The assessment considered the current controls and pointed out important gaps that affect data protection, cloud configuration, the software supply chain, third party dependencies, human error and social engineering, incident response readiness, regulatory compliance, and customer trust after an incident.

Based on the results, the thesis suggests a short list of treatment strategies that can be quickly put into action in a setting with limited resources. A total of five proposals are given top priority because they will have the biggest effect with minimal resource cost to put into action. These are quarterly tabletop exercises with a one page communication playbook, enabling cloud guardrails and monthly access reviews, a simple component inventory with automated dependency alerts, continuous security awareness with a no blame reporting culture, and a prepared “customer trust pack” for clear communication after an incident.

The thesis delivers actionable strategies that a small IT startup can use to strengthen financial resilience against possible cyber incidents. The purpose of this thesis is to help companies like Company X to understand the financial risks related to cyber threats. Strategic planning and flexibility are essential, as competitive advantage will favor teams that adapt quickly while preserving customer trust.
Keywords: Risk Assessment, IT Security, Small and Medium Enterprises

Contents

1 Introduction

As the digitalization of businesses increases, cybersecurity risks can impact the financial stability of companies also increase. These risks are particularly dangerous to companies that operate with small teams and limited resources such small and medium enterprises. For companies such as these, any successful cyber attack can cause substantial financial loss. This situation can be due to service disruptions, data leaks, regulatory fines and reputational damage. Although the growing danger is ever present, many companies prefer to prioritize growth and product development over structured risk management.

Company X is a Berlin-based technology startup offering a cloud-based platform that enables companies to conduct online focus groups, in-depth interviews and usability testing with AI-powered transcription and analysis. This thesis aims to examine cybersecurity threats that can cause financial risks in a small IT company context, using Company X as an example. Company name has been anonymized and will be mentioned as Company X in this thesis. In this thesis report, ChatGPT has been used to edit the language of the text and make the text smoother.

1.1 Objectives of the Thesis

According to LaMacchia and Selznick (2108, 224), small IT companies often function with no formal frameworks for assessing financial risks due to cybersecurity threats. Despite being highly dependent on digital infrastructure, these companies typically lack the dedicated personnel, structured processes, or financial risk mitigation strategies that can be found in larger organizations. LaMacchia and Selznick (2018, 224 225) also state that, due to the tendency to overlook the possibility of a cyberattack, smaller businesses have a high possibility of being targeted.

Small IT startups operate in a risky environment since even a single cybersecurity incident can quickly cause a critical financial crisis. According to Company X CTO, CTO of Company X, even a single data breach could cause “irreparable financial and reputational damage,” given the lean operational models and trust based business dependencies of such companies. Cyber attacks like service outages, phishing and third party failures are a constant threat yet a structured financial risk analysis is often missing due to time constraints, lack of awareness or limited resources.

The main objective of this thesis is to explore cybersecurity related risks that can create financial risks within the context of small IT startup. The thesis aims to create an understanding of these risks and find out how they can be managed. By creating a structured

process of the assessment, it aims to provide insight into how small technology driven enterprise can increase their financial resilience and decision making capability.

1.2 Scope, Context and Risk Criteria

This thesis focuses on identifying and assessing financial risks that arise from cybersecurity threats in small information technology companies, using Company X as an example case. The assessment is limited to risks that directly or indirectly affect the company's financial situation in any way due to cyber incidents. Long or short term consequences are also included in the scope of this thesis hence no risk will be excluded due to its distant time of occurrence. These incidents can and not limited to be data breaches, ransomware attacks, denial of service attacks or third party service failures.

While the cybersecurity landscape includes legal, technical and reputational dimensions, the scope of this thesis is narrowed to the financial consequences of these events, such as loss of revenue, regulatory fines, increased recovery costs, legal liabilities and loss of investor confidence. Company X operation exists in a digital service environment hence it is heavily relied on data integrity, customer trust and cloud infrastructure which makes it particularly vulnerable to disruptions with financial consequences.

The risk assessment is guided by the general framework that can be found in ISO 31000 (Risk Management Guidelines) and ISO/IEC 27005 (Information Security Risk Management). These frameworks inform how risks are defined, evaluated, and prioritized in the context of a small IT business. The following criteria are graded with high, medium and low parameters:

I. Likelihood: The estimated probability that a particular cybersecurity threat will materialize
II. Impact: The potential financial damage if the event were to occur
III. Vulnerability: How exposed or unprepared the organization is for each type of threat

This thesis is purely limited to providing proposals for the mitigation of discovered risks for the Company X. There are no requirements for action for the Company X in the scope of this thesis. Acting on any recommendation for the proposed strategies is on company's prerogative.

The assessment does not aim to create a fully quantitative financial risk model but rather offers a practical, structured method that can assist decision making in similarly positioned startups. The goal is to make risk awareness a present process in a resource constrained environment where formal risk functions may not exist.

1.3 Key Concepts and Definitions

Aim of this section is to provide definitions that will be used throughout the thesis. These definitions are meant to help clarify the scope of the analysis and make it easier to understand when interpreting the results.

I. Cybersecurity Risk: An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (National Institute of Standards and Technology 2025).

II. Financial Risk: Any risk that can cause a direct or indirect loss of financial stability. In this thesis financial risks that are included are the outcomes of cybersecurity threats. These involve but are not restricted to loss in revenue, penalties, legal expenses and harm the trust from investors or customers.

III. Risk Assessment: This methodical approach is used to recognize, assess and rank risks. This thesis applies concepts from ISO 31000 (Risk Management – Guidelines) and ISO/IEC 27005 (Information Security Risk Management) for evaluating financial risks related to cybersecurity in small IT firms.

IV. ISO 31000: An international standard that provides pathway on managing risk encountered by organizations. It outlines principles, a framework, and a process for risk management that can be used by any type of organization (ISO 2018).

V. ISO/IEC 27005: A standard specifically focused on information security risk management. It supports the broader ISO/IEC 27000 series and provides detailed guidance on identifying, assessing, and treating cybersecurity risks (ISO 2022).

VI. IEC 31010: A document that gives guidance on the selection of methodology of various techniques that can be used to increase the efficiency of understating risk. (ISO 2019)

VII. Vulnerability: A weakness in systems, practices, or infrastructure that increases the likelihood or potential impact of a cybersecurity threat.

VIII. Startup / Small IT Company: A company that is not very big and doesn't have many resources, working in the digital or software area. These types of businesses usually grow quickly, operate with small teams or simple structures and depend a lot on cloud technology and services from other companies.

IX. SME (Small and Medium sized Enterprise): The European Commission defines a larger category, which includes businesses with less than 250 employees and yearly turnover of not more than €50 million. IT sector SMEs frequently face the same cybersecurity and financial risk issues as startups do (European Commission 2020).

2 Theoretical Framework

The theoretical framework of this thesis is based on ISO 310000:2018 Risk Management Guidelines and ISO/IEC 27005/2018 Information Security Risk Management, since these are internationally recognized standards which provide a solid foundation for the assessment of cybersecurity related financial risks. In addition, the framework is supported by academic and legal literature on cybersecurity risk governance, financial exposure in small enterprises, and organizational resilience. Furthermore, news and articles related to IT industry, public records form German Government and European Union, and lastly IEC 31010:2019 risk assessment techniques are present to support the validity of the thesis.

2.1 Risk Management Frameworks

ISO 31000 defines risk as “effect of uncertainty on objectives” which includes both possible outcomes of positive and negative (ISO 2018, 1). While risk may involve opportunities, this thesis focuses primarily on threats that can lead to financial damage in small IT startups. This thesis aims to find the possible negative outcomes derives from cybersecurity threats that may endanger Company X’s future as a business.

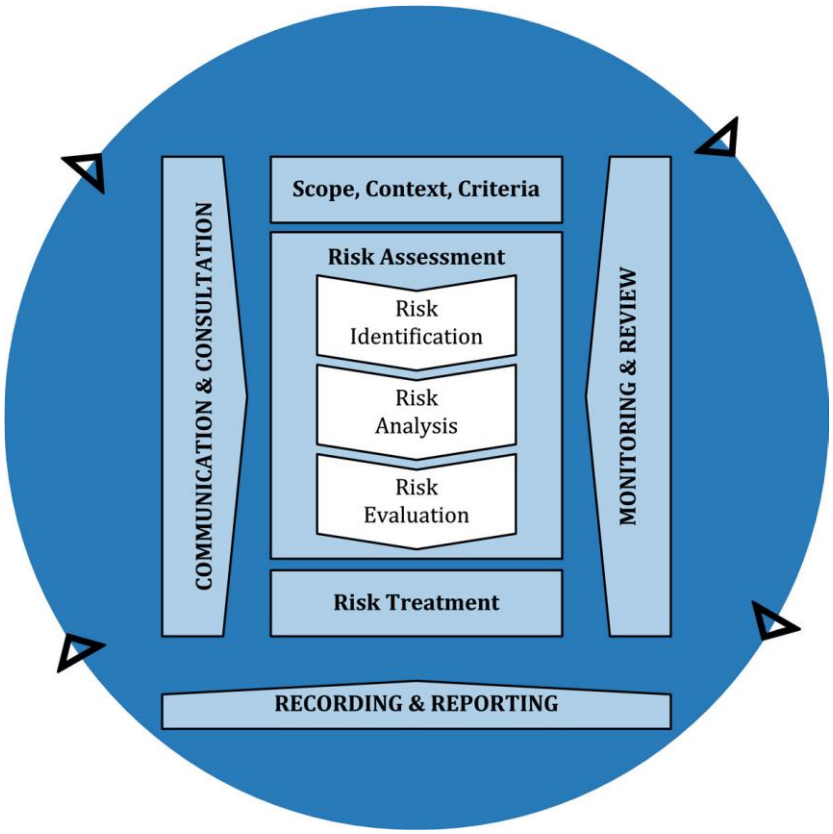

Figure 1: ISO 31000 Process (ISO 2018, 9)

ISO 31000 describes that successful handling of risk is not a one off job, but an ongoing and repetitive method which makes part of decision making and every layer of the organization. In accordance with what's set out in this standard, managing risk involves planned actions to guide and oversee a company concerning danger (ISO 2018, 1). This process, as seen in Figure 1, starts by setting up the context, then in an orderly manner identification, analysis, evaluation and treatment. It also includes observing, checking and conveying the results (ISO, 2018, 13).

To support risk identification and evaluation, ISO/IEC 27005:2022 offers a framework specifically for information security risk management. It emphasizes the importance of tailoring the risk assessment process to the information systems and operational context of the business. In the case of small IT companies, this means accounting for the organization's specific architecture, digital dependencies, and exposure to cyber threats (ISO 2022).

Although ISO 31000 provides a guideline for risk assessment, it does not mention techniques to increase the risk assessments efficiency. IEC 31010 complement ISO 31000 in this regard by providing techniques. It states that the choice of methods should match the decision making needs and available data within the organization (ISO 2019, 16). For small IT companies where quantitative data may be limited, qualitative approaches like expert judgement, checklists or brainstorming are more likely to produce valuable insights into the likelihood and impact of possible events.

A critical definition on this framework is risk appetite which is defined as the level and type of risk an organization is willing to accept in pursuit of its goals (ISO 2019, 14). According to LaMacchia and Selznick (2018, 225) SMEs often operate with higher tolerance of risk due to their product growth orientated strategies even though a single cyber incident may mean a catastrophic financial consequence. Therefore, risk evaluation in this context must consider not only the severity of potential losses but also the organization's capacity to withstand them.

Risk assessment, according to ISO 31000, has three main parts: these parts can be observed in Figure 1, are risk identification, risk analysis and risk evaluation (ISO 2018, 11–12). In this thesis, the risk assessment process follows this model to build a structured understanding of cybersecurity threats that have financial implications. The objective is to give decision makers in small IT companies insights they can act on that make them more resilient and cut down on their exposure to financial instability that may derive from cyber threats.

2.2 Cybersecurity Risk and Financial Exposure

Cybersecurity risk in this thesis represents consequences that derive from cyber attacks that cause financial instability for the SMEs. These risks can be listed as potential for disruption,

data loss or business operational failure caused by attacks or system vulnerabilities. For SMEs, including IT startups, face these risks more because they don't have enough resources, rely on third party service providers, and don't have enough internal expertise (Tetteh 2024). AccuantancyEurope (2022) says that small and medium sized businesses (SMEs) are some of the most common targets of cyberattacks. This is because their defenses are often not as strong as those of larger businesses, which makes them easy targets for opportunistic attackers. Phishing, data breaches, and ransomware are all examples of attacks that can quickly put the business's core operations and customer data at risk, which can have terrible effects.

Cyber incidents that cause direct or indirect financial losses can put companies at risk of losing financial stability. These consequences could include system downtime, the cost of recovery, legal liabilities, fines from regulators, and damage to the company's reputation. According to Cobos and Cakir (2024), the anticipated cost of cyber incidents may far exceed the initial estimations particularly for small businesses lacking contingency reserves or insurance coverage. When small and medium sized businesses aren't ready for emergencies, they increase their financial risks and their long term business continuity.

2.3 Risk Awareness in Small and Medium Enterprises

Risk awareness is another idea that is often ignored because of a lack of resources, formal procedures for managing risk, and the belief that the organization is "too small to target" (Tetteh, 2024, 238). Even though there is more proof that opportunistic cybercriminals often go after small and medium-sized businesses (SMEs), many people still think that the risk is low. This false belief makes people careless about planning and investing in security, which could cost them financial stability because they weren't ready (Tetteh 2024).

3 Methodology

The main method used in this thesis is qualitative case based risk assessment, which is done by combining a document analysis and a targeted literature search to create the theoretical framework. As Creswell (2017, 22) notes, qualitative research is particularly effective in situations where the goal is to understand “the meaning individuals or groups ascribe to a social or human problem,” making it ideal for examining risk awareness and management behaviors in SMEs. The knowledge base foundation includes international standards, academic publications, cybersecurity checklists, and publicly available policy guidance related to SMEs, cybersecurity, and financial risk management. Financial risks emerging from cybersecurity threats in small IT company is identified, analyzed and evaluated, using Company X as a case company.

The materials used to build the foundation of this thesis are ISO 31000 (Risk Management Guidelines), ISO/IEC 27005 (Information Security Risk Management) and IEC 31010 (Risk Assessment Techniques). These materials give a solid foundation to the thesis for identifying and assessing risk scenarios. Supplementary insights are drawn and not limited to, from Accountancy Europe's (2022) SME Cyber Resilience Checklist and the World Bank's economic impact report on cyber incidents (Cobos & Cakir 2024), which better define financial exposure at the SME level. In addition, interview with industry expert, input from Company X's leadership has been considered to interpret risks in both operational and practical context.

3.1 Document Analysis and Literature Research

This thesis uses a qualitative approach and puts document analysis and targeted literature search to build the theoretical framework as its center. The main materials used in this thesis are international standards such as ISO 31000, ISO/IEC 27005, and IEC 31010. The following globally accepted guidelines provide a solid foundation for efficient risk management in both general and information security contexts. Furthermore, documents related to the General Data Protection Regulation (GDPR), relevant German legislation affecting IT operations, and industry specific guidance such as articles, papers, news and reports within the IT startup landscape were reviewed. Materials used in this thesis are chosen for their practical relevance, regulatory significance and most importantly for their applicability to financial and cybersecurity risks within small IT companies.

The choice of document analysis is based on its ability to extract meaning, patterns, and insights from policy texts, standards, and published frameworks that are important to comprehend most efficient methods in risk management. Document analysis is especially suitable for topics involving regulatory structures or standardized processes, where interpretation of written guidance forms the basis for action (Bowen 2009). Also, Bowen (2009, 27) defines document analysis as "a systematic procedure for reviewing or evaluating documents—both printed and electronic (computer based and Internet transmitted) material" and it is highly effective in understanding organizational practices and policy frameworks.

On the other hand, targeted literature search to build the theoretical framework is used to position this thesis within the broader field of financial risk, cybersecurity threats and SME risk management. It is used for identifying challenges that are known, relevant risks and common gaps in how financial risk due to cybersecurity threats is handled. Creswell (2017, 41) says qualitative research is most effective when the researcher aims to understand how individuals or organizations interpret and respond to complex issues in context. In this situation, the aim is to understand how small IT companies see and react to financial risks caused by cyber incidents, and literature helps put this question with support from academic and industry perspectives.

Used together as the main research method, document analysis and literature research gathers information from various sources to enhance the credibility of this thesis. Furthermore, it allows a better understanding of Company X's financial risk environment due to cyber threats. By using both methods, not only it increases the interpretation of findings but also supports the credibility of practical recommendations that reflect both best practices and real world limitations experienced by small IT companies operating under limited resources.

3.2 Interview

Interview method is a widely accepted method of qualitative data collection, particularly if the goal is to gain understanding of the experiences, attitudes and related knowledge that may not be able to find through available documents (Gill, Stewart, Treasure, Chadwick 2008). The reason a semi-structured interview was chosen is because it can get qualitative information that might be hard to find in official documents. Kallio, Pietila, Johnson, and Kangasniemi (2016) assert that semi-structured interviews provide a flexible yet systematic method for obtaining detailed information, allowing researchers to address intricate issues while preserving sufficient structure to ensure uniformity across interviews. Semi-structured interviews are also good for research situations where you want to learn about the experiences, practices, and context-specific understandings of industry experts (Kallio et al. 2016).

In this thesis, semi structured interview was conducted with the Chief Technology Officer (CTO) of Company X. The interview was carried out in July 2025, and the main goal of the interview was to better understand and analyze information collected through document analysis and literature research by comparing findings with the subject expert knowledge and experience.

The interview questions are as follows:

- Could you briefly introduce yourself and the company?
    - What is Company X's area of business?
    - How long has the company been operating?
    - What type of clients or industries does Company X serve?
- Have you experienced or observed any specific types of attacks, such as DDoS, phishing, or social engineering?
    - Which of these threats caused the most disruption or concern?
    - What technical issues have been the main sources of vulnerability (e.g., misconfiguration, insecure development pipeline)?
    - How does human error factor into cybersecurity risks at Company X?

- How does Company X prevent and manage cybersecurity threats?
    - Have you experienced any major security incidents so far?
    - What is the key preventive steps your company takes (e.g., code review, pen testing, documentation)?
    - What challenges do you face when implementing frameworks like ISO 27001?
    - Who is responsible for defining the cybersecurity strategy within the company?
    - Do you follow a particular framework (e.g., ISO 27001) or rely mainly on best practices?
- What tools, policies, or procedures do you use to protect against cybersecurity threats?
    - Can you give examples of internal policies or processes (e.g., access control, encryption, onboarding/offboarding)?
    - How do you ensure employees follow best security practices?
    - How do you monitor or audit compliance with these practices?
- How do financial risks influence your cybersecurity decisions?
    - How do you evaluate the financial impact of potential cybersecurity incidents?
    - Do you estimate direct and indirect costs (such as downtime or client loss)?
    - How is the impact categorized (e.g., low, medium, high)?
    - How do you financially prepare for a worst case scenario? (e.g., insurance coverage)
- What role do external requirements such as GDPR, or industry standards play in shaping your cybersecurity and financial risk management?
    - Have compliance requirements affected your budgeting or planning?
    - Do German regulations differ from EU wide GDPR in your experience?
    - Have you encountered any fines or audits from regulators?
    - How do these regulations influence your company's operational decisions?
- What do you see as the biggest financial risks from cybersecurity in the next few years for small to medium enterprises?
    - How do you balance user friendliness with strong security measures?
    - Are emerging threats like AI driven attacks a concern for you?
    - Do you think insurance policies or regulations will change to address AI related cybersecurity risks?

3.3 Brainstorming and Risk Identification Process

Brainstorming was used in this thesis as a complementary qualitative method to support the risk identification process. The aim of the brainstorming session was to merge the findings of

various information collection methods with the open and unrestricted generation of ideas related to cybersecurity threats that causes financial risks within the context of a small IT company. According to Wilson (2013, 2–7), brainstorming is a creative group process designed to generate ideas for solving problems or improving outcomes, and its success depends on encouraging free thinking without immediate evaluation or criticism of suggestions.

In the context of this thesis, an informal brainstorming session was conducted. The goal was to map out cybersecurity related financial risks based on industry experience and observations. The session began with individual reflection phase and continued with joint session where generated ideas were pooled together and discussed. IEC 31010:2019, which notes that individuals tend to contribute more diverse ideas when working alone, while group settings can unintentionally limit creativity due to conformity or social inhibition (IEC 31010 2019, p. 41). Combination of both phases produced a session where broad coverage of ideas were produced and enabled reflection from multiple perspectives.

Brainstorming was very helpful for connecting practical ideas with theoretical models. It helped create the risk list used later in risk assessment and allowed finding both expected and unforeseen risks particular to Company X's business situation.

3.4 SWOT Analysis of Company X

Swot analysis was selected due to its ability to clarify and organize findings from interview and brainstorming session as a strategic structured tool in the context of financial risks related to cybersecurity threats. According to Pickton and Wright (1998) SWOT enables firms to map internal capabilities and external circumstances in a simple yet comprehensive way that supports decision-making. According to Puyt, Lie and Wilderom (2023), SWOT's strength lies in its ability to bridge descriptive insights and strategic action by helping organizations convert qualitative information into targeted priorities.

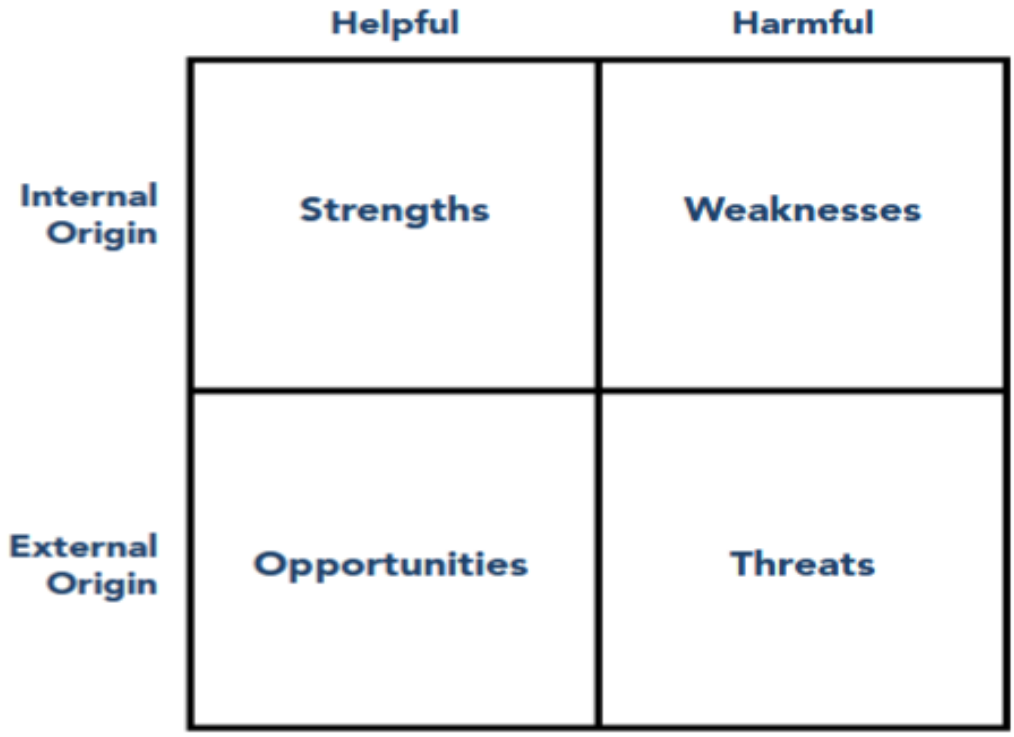

Figure 2: SWOT Analysis (Swot Analysis 2013, 6)

For the purposes of this thesis, the SWOT method connects qualitative data collection with a structured way to assess risk. Company X is a small IT company, and this gives them a flexible way to capture both operational realities and outside threats or opportunities. The insights gained from previous methods, including interviews and brainstorming sessions, are structured into a strategic overview that displays internal strengths and weaknesses alongside external opportunities and threats. The study uses SWOT to make sure that the results are not only descriptive but also useful for Company X's business setting and limited resources.

3.5 Risk Assessment Criteria and Evaluation Framework

This thesis uses a structured risk assessment approach to categorize and prioritize cybersecurity related financial risks in a small IT startup. The significance of each identified risk is determined by evaluating its likelihood of occurrence and potential financial impact on the company’s operations, using a three level severity system which are low, medium, or high. This matrix is illustrated in Table 1, page 15.

	IMPACT				
LIKELIHOOD	Severe (5)	Major (4)	Moderate (3)	Minor (2)	Negligible (1)
Very Likely (5)	High	High	Medium	Low	Low
Likely (4)	High	High	Medium	Low	Low
Possible (3)	High	Medium	Medium	Low	Low
Unlikely (2)	Medium	Medium	Low	Low	Low
Very Unlikely (1)	Low	Low	Low	Low	Low

Table 1 Risk Significance Matrix, 2025.

The impact level refers to how significantly a cybersecurity event could affect the company's finances and business continuity. These categories are detailed at Table 1, page 16.

Level	Impact	Expected Consequences
1	Negligible	Minimal or no financial loss; no effect on operations
2	Minor	Slight financial disruption; small impact on daily business activities
3	Moderate	Noticeable financial strain; potential to disturb core operations
4	Major	Major economic consequences; likely to cause operational slowdowns or temporary outages
5	Severe	Critical financial impact; can significantly disrupt or halt business operations

Table 2 Risk Impact Levels, 2025.

The likelihood classification reflects how probable it is for a particular cybersecurity risk to occur based on industry patterns and organizational context. These classifications are listed at table 2, page 16.

Level	Impact	Expected Consequences
1	Very Unlikely	The event is not expected within the next 10 years or may never occur; no known prior occurrence
2	Unlikely	Possible once in 10 years; rare in industry; limited or no historical occurrence
3	Possible	May occur within the next 10 years; at least one similar case known in comparable organization
4	Likely	Expected to occur every few years or more frequently; prior incidents observed in the field
5	Very Likely	Anticipated occurring repeatedly within a year; trend observed across small IT companies

Table 3 Risk Likelihood Classification, 2025.

A formula has been used in this thesis to be able to prioritize financial risks caused by cybersecurity threats. Qualitative risk analysis commonly evaluates risks by combining estimates of likelihood and impact, which together provide a structured basis for comparing and ranking different risk events (Tiusanen 2018, 463–465). While standard approach is to apply the formula "Risk = Likelihood × Impact", but this thesis adopts a modified version of "Risk = Impact^2 × Likelihood". This change aims to address the more vulnerable aspect of SMEs regarding increased potential consequences. This perspective is supported by Company X's CTO Company X CTO, who emphasized during the interview that "even one cybersecurity incident may be critical for a company of our size.". The risk value range is illustrated in table 4, page 17.

Severity	Risk Value Range	Interpretation & Recommendation
Low	0–25	Negligible to minor impact or low probability; mitigation is optional; periodic review may suffice
Medium	26–63	Either impact or likelihood is moderate to major; mitigation and monitoring are recommended
High	64–125	Severe consequences and/or high probability; mitigation, control, and regular risk tracking are highly recommended

Table 4 Risk Value Thresholds, 2025.

3.6 Risk Mitigation Approach

This thesis recommends risk treatment strategies for the identified financial risks due to cybersecurity threats present in Company X environment. These suggestions are meant to lower Company X's financial risk by either stopping certain risks from happening or making the possible effects less severe. The risk evaluation framework described earlier in this thesis is the basis for each recommendation. It was made with Company X's environment in mind, which includes the operational characteristics and limitations of a small IT company.

The recommended treatment methods aim to achieve one or more of the following outcomes:

- Reduce the likelihood of the risk materializing
- Lower the severity of financial consequences
- Eliminate the risk by removing the underlying vulnerability
- Avoid the risk entirely by altering specific business activities or dependencies
- Transfer the risk to third parties (e.g. through cyber insurance or contractual arrangements)
- Accept the risk where it is deemed tolerable within the company's strategic goals or resource limitations

Improvements to existing measures may involve strengthening enhanced third party monitoring, strengthening data protection methods, introducing multi layered access controls or creating incident response plans. In areas involving sensitive customer data or critical cloud infrastructure, new treatment actions may also be recommended.

Lastly, continuous activities such as regular risk reviews, policy updates and awareness initiatives are proposed to further embed continuous risk management into the Company X’s culture.

4 Results

This section of the thesis represents all the findings of methodologies used in search of financial risks derived from cybersecurity threats. Brainstorming session and SWOT analysis outcomes followed by risk assessment results and lastly found risks will be put through the risk evaluation matrix. Treatment methods for risks will also be present in the respected sections.

4.1 Brainstorming and SWOT Analysis of Company X

This section presents the outcomes of the brainstorming session and the SWOT analysis conducted to identify key cybersecurity related financial risks relevant to Company X. The goal was to find out the internal and external factors that influence the company and to gather perspectives from leadership to support the assessment process of potential threats. The brainstorming session was conducted in September and SWOT analysis was done soon after.

4.1.1 Brainstorming Outcomes

The brainstorming session was conducted on 5th of September 2025. The session highlighted that Company X is a small IT company with a lean team and limited resources that faces several connected risks in its digital operations. Among the many cybersecurity threats, the most prominent one that stood out in this session and interview with potentially devastating consequences was the risk of data breach (Company X 2025).

Among the other risks, the key highlights were misconfiguration of cloud infrastructure, insecure software development pipelines, and overreliance on third party service providers. In the absence of a full time security personnel, these risks are mainly considered as technical issues in a small It company, rather than as risks. In addition, risks such as service downtime, documentation burdens from compliance, and the usability–security trade off were also raised as areas of concern. On the financial side, session and the interview uncovered that reputation loss could almost directly translate to revenue loss, given the company's B2B SaaS (Business to Business Software as a Service) model and trust based customer relationship. Compliance requirements for German Federal Data Protection Act (BDSG) which is specialized version of GDPR for Germany and its associated costs noted as strains for the company resources. Finally, one critical risk was highlighted which was the AI driven attacks due to obsolescence of current bot protection tools like CAPTCHAs. This new threat was pointed out as emerging issue that requires monitoring even with limited resources.

Among the many discussed ideas, these outcomes were decided as the most relevant to Company X's current environment and helped formulate the basis of the SWOT analysis and assisted the risk identification process in later stages of this thesis.

4.1.2 SWOT Analysis

Strength	Weakness
• Lean, agile team capable of rapid development and adaptation. • Cloud-based service offering with scalable infrastructure; supports remote collaboration and flexible deployment. • Niche position in the market (online focus groups, usability testing) allowing premium trust-based client relationships. • Leadership acknowledges cybersecurity and its financial implications, suggesting a proactive awareness.	• Minimal dedicated cybersecurity staff or formal SMS (Security Management System). • High dependency on third-party cloud providers and external services, increasing uncontrolled risk exposures. • Limited financial reserves and risk-absorption capacity typical of small IT companies. • Lack of incident response testing, documentation and formal compliance frameworks beyond minimal requirements.
Opportunities	**Threats**
• Growing demand for secure, privacy-compliant SaaS platforms, particularly in regulated European markets (GDPR, data localization). • Potential to differentiate on cybersecurity by offering “secure by design” positioning and leveraging this as a competitive advantage. • Availability of cyber-insurance, regulatory funding, and EU security grants that startups can leverage for resilience improvements. • Emerging AI-driven attack vectors provide an opportunity for Company X to invest early in advanced defenses and gain lead over less prepared competitors.	• Data breach or leak could cause severe financial, legal and reputational consequences for Company X’s trust-based business model. • Cloud misconfiguration, software supply-chain vulnerabilities, and third-party failures constitute immediate and heightened risk vectors. • Increased regulatory scrutiny (especially in Germany and EU) with high-penalty regimes, posing legal and financial risk from non-compliance. • Reputation loss can rapidly lead to revenue decline, client churn, and long-term business damage given the small startup size.

Table 5 SWOT Analysis, 2025 (Swot Analysis 2013).

SWOT analysis was done on 6th September 2025 which was a day after brainstorming session. Table 5 on page 20 represent all the findings of the analysis.

Company X's key strengths lie in its agile team and its possibility for rapid development and adaptation. Its cloud-based design makes it easy to grow and change, which lets it reach more customers. The platform's AI-based features also include advanced transcription and usability testing tools, which give it an edge in the niche B2B SaaS market, where there is a lot of demand for remote research tools. Most importantly, the company's leaders are proactive in their understanding of cybersecurity issues, which makes them more aware and ready for strategic situations.

Company X has some structural limitations, even though it has a strong posture. It doesn't have a formal system for managing cybersecurity, which makes it more open to advanced threats. Heavy reliance on a third-party cloud provider causes a diminished control in data security or system uptime. Due to small IT companies' environment, any cyber incident could cause serious financial instability. Finally, the company is at risk because it doesn't have any emergency preparations, like incident response procedures.

There is growing demand for reliable SaaS platforms, especially in the EU where data protection and localization laws are quite strict. This demand gives Company X an opportunity to stand out as a secure by design provider. Funding opportunities like cyber insurance and EU startup security grants are also potential growth accelerators. Investing in advanced security practices early in companies' growth could let Company X get ahead of competitors as AI driven threats go up across the industry.

Threats include the factors that cause significant consequences such as critical financial instability, operational downtime and reputational loss. These threats are and not limited to data breaches, cloud misconfiguration, software supply-chain vulnerabilities, and third-party failures. One constricting factor to consider is with the ever expending digitization, so does the regulations for protecting information. This can create new compulsory legal actions that requires staying vigilant for any update.

4.2 Identified Cybersecurity Related Financial Risks in Company X

The cybersecurity related financial risks relevant to Company X have been identified through a combination of various data sources. These include the semi structured interview with CTO Company X CTO, brainstorming session, document analysis and literature research of academic research and professional risk management frameworks such as ISO 27005, ISO 31000, and IEC 31010.

The following risks have been identified as potentially having financial consequences for Company X:

- Data Breach / Data Leak
- Cloud Misconfiguration & Infrastructure Security Failures
- Software Supply Chain Vulnerabilities
- Third-Party Service Outage or Provider Security Failure
- Human Error & Social Engineering
- GDPR or Regulatory Non-Compliance
- Inadequate Incident Response Preparedness
- Loss of Customer Trust Following a Security Incident

4.2.1 Data Breach / Data Leak

4.2.1.1 Risk

Data breaches and data leaks present one of the most crucial cybersecurity threats to Company X. In the context of Company X's cloud-based SaaS model, which handles sensitive research data and client transcripts, a single incident could trigger a cascade of financial, legal, operational and reputational consequences. In the interview Company X CTO especially pointed out that a data breach incident in his words "Of course one of the huge issues is data leak. That's a Horror Story. And of course, there could be other issues that could happen also like the downtime. Downtime is also bad but not so bad as a data leak" (Company X CTO 2025).

Severity of this risk for SMEs is strongly supported by academic and institutional literature. A study titled "Revealing the Realities of Cybercrime in Small and Medium Enterprises" by Arroyabe, Arranz, Arroyabe, and Arroyabe (2024b) found that 46% of all successful cyberattacks on small businesses involved stealing or exposing data. This makes data breaches the most common and costly type of incident. A systematic review conducted by Rombaldo Junior, Becker, and Johnson (2023) demonstrates that SMEs are uninformed, underfunded, and ill prepared, with more than 60% lacking the ability to detect a breach in real time, thereby substantially prolonging exposure duration and expenses.

The effects on financial stability are quite large. The World Bank reported that cyber incidents cost small and medium sized businesses (SMEs) 30–40% more than they do compared to large businesses. This is due to SMEs being less resilient and lacking backup systems environment (Cobos & Cakir, 2023). A 2025 scoping review indicates that 71% of SMEs encountering a significant data breach endure extended revenue loss, with one in five failing to achieve financial recovery (Awan, Alam & Kamran 2025). These findings underscore the

probability of a significant breach and its severe potential impact on the Company X. For Company X, three things make this risk even worse:

- The customer research data makes any breach a contractual and reputational crisis.
- Strict GDPR requirements, especially in Germany, which impose high financial penalties.
- Dependency on third-party cloud services, meaning any upstream failure can lead directly to accidental exposure.

Given these internal and external considerations, a data breach must be treated as a high-impact, high-priority risk within Company X's financial risk assessment framework.

4.2.1.2 Treatment

Company X already applies mitigation strategies thanks to its approach to data security such as ISO 270001 compliance, manual reviews and version controls and basic cloud hygiene. Recommended treatments are for expanding the present protection layers and adding new ones to increase their stance on data security.

Rombaldo Junior et al. (2023) note that technical training is one of the most effective treatments for reducing data breach risks in SMEs. Although Company X is a small company with highly trained employees, training method is still a highly effective method. Training would be a reminder for those who are knowledgeable in the area and new information for those who were not aware hence all employees handling sensitive data should undergo targeted privacy by design and secure coding training, with a strong emphasis on GDPR Article 25 and OWASP principles. Free platforms such as OWASP Juice Shop or Mozilla's Secure Coding Guidelines provide zero cost resources. This helps reduce the risk of data exposure through insecure software development practices.

According to NIST Special Publication 800 207, Zero Trust Architecture (ZTA) is a cybersecurity paradigm focused on resource protection and the premise that trust is never implicit; it must be continually evaluated (Rose, Borchert, Mitchell & Conelly 2020, 4). To further define meaning that no user or system is automatically trusted. Instead, every access request must be validated in every step based on identity, context, and other risk factors before granting access to data. According to Cobos et al. (2023), zero trust adoption significantly reduces breach dwell time and lateral movement risks, especially in remote/hybrid teams. Implementing ZTA may seem overkill for a company of Company X's size, but recent developments make it achievable through managed cloud platforms. For example, Google Cloud BeyondCorp or Azure AD Conditional access allows users to device and identity aware controls allowing that any movement of data can be subjected to policy based approval.

Awan, Alam & Kamran (2025) note that third party SOC as a Service solutions are now affordable and effective for SMEs lacking internal security operations. Company X should consider contracting a Managed Security Service Provider (MSSP) to provide breach detection and response alerts outside business hours. Even a basic log anomaly monitoring agreement can provide crucial early warning before a leak becomes critical.

A creative and lightweight strategy is the use of honeytokens which is defined as digital resources that are purposely designed to be attractive to an attacker but signify unauthorized use by Vaideeswaran (2025). It is a decoy data entry planted within databases or log systems that trigger silent alerts when accessed. Honeytokens are considered a low cost, high reward defense tool that is particularly suited for companies with limited detection capabilities (Arroyabe, 2024a). Company X could place synthetic "customer accounts" or "fake research files" with embedded alerts to detect unauthorized scraping or exfiltration.

Lastly, according to Amosh and Khatib (2024), transparent communication regarding both cybersecurity measures taken and any cyber attack enhances the overall trust of the company's readiness. For the overall readiness also preparing for inevitable worst case scenarios and to gain customer trust and, Company X could run a mock breach simulation and publish a redacted post incident response plan. Transparency around cybersecurity preparedness can enhance credibility and customer confidence.

4.2.2 Cloud Misconfiguration & Infrastructure Security Failures

4.2.2.1 Risk

As a small IT company, Company X's reliance on cloud services for its SaaS offering such as handling client-data, AI transcription, and storage across multiple third-party cloud providers, the company faces an enlarged attack surface. During the interview, the Company X CTO noted that "misusing cloud infrastructure can lead to exposed data," highlighting the practical immediacy of the threat (Company X CTO 2025). Thanks to Company X's awareness of the threat and attitude towards such possibilities, it boosts the company's overall posture against such threats.

This is a generally known and often neglected risk in IT industry. A 2025 report found that 39% of cloud-related incidents in SMEs were traced to misconfigurations. This highlights how such errors can directly lead to financial exposure (Rapley 2025). Also, according to Ashwood's analysis of cloud breaches (2023), common misconfigurations such as disabled logging, excessive IAM permissions, and publicly accessible storage buckets remain top vulnerabilities for attackers. Furthermore, broader SME studies shows that cloud computing adoption introduces risks of "lack of control" and "security/privacy concerns" that especially affect smaller organizations (Kolli 2025). Finally, research on software misconfiguration shows that

over 800 real-world misconfiguration issues were analyzed, and many were linked to cloud service setup errors leading to security incidents (Lui, Zhou & Zhang 2024)

For Company X, this risk is especially relevant because:

- Their business model depends on cloud infrastructure and rapid deployment, increasing pressure to prioritize release speed over security controls.
- The reliance on third-party providers means Company X cannot directly control all infrastructure layers; misconfigurations can arise upstream and propagate downstream.
- As a small IT company, Company X is vulnerable to configuration drift.
- Any infrastructure failure or data exposure can lead to operational downtime, customer attrition, regulatory liability and thus significant financial impact.

Taking these reasons into account, cloud misconfiguration and infrastructure security failures as a high-priority risk for the Company X. This is mainly because the business model which deals with sensitive client information on a regular basis.

4.2.2.2 Treatment

To address the risk of cloud misconfiguration and infrastructure failures, three recommendations are presented. The company's current level of usage of third party cloud platforms and its limited internal security automation, which were highlighted during the interview, are the reasons for the following recommendations.

Cloud Security Posture Management (CSPM) solutions automate the process of detecting misconfigured resources in cloud environments. For small IT firms like Company X, integrating lightweight CSPM tools can significantly reduce manual oversight requirements. Ashwood (2023) states that CSPM tools are quite important for preventing the common misconfigurations that lead to breaches because they offer real time monitoring, compliance auditing and remediation support.

By embedding security validation checks into the development pipeline, Company X can catch infrastructure as code errors or insecure configurations before they reach production. They are already doing such security checks with branch testing and code reviews but tailored automation for such configuration checkup increases the possibility of finding the mishap if present. Liu et al. (2024) mentions the critical importance of identifying misconfiguration errors early in the software lifecycle, noting that cloud related misconfigurations were often introduced through tools or default templates.

Misuse of permissions is a critical misconfiguration issue. Rapley (2025) explains that small businesses often grant overly broad access to speed up development. Enforcing least privilege

reduces lateral movement and limits damage in the event of an incident. Company X already applies principle of least privilege in its core. To further mitigate the issue company should regularly audit and enforce the principle of least privilege, ensuring that users and services only receive the minimum access necessary. This reduces the blast radius in case of credential compromise or internal misuse.

These treatment strategies are designed to be low overhead, high impact measures suitable for Company X. The overall goal is to strengthen the infrastructure security and reduce the complexity of risks related to cloud misconfigurations without sacrificing agility.

4.2.3 Software Supply Chain Vulnerabilities

4.2.3.1 Risk

When external code, libraries, components, or services are inserted into a company's product or infrastructure, they may turn into a target for attacks. This is called a software supply chain vulnerability. This risk is a direct financial and operational concern for a small IT company like Company X, which builds and deploys a SaaS platform using a lot of open-source and third-party tools. During the interview, Company X's CTO acknowledged that "third-party library vulnerabilities inherited into the product" are a key worry, acknowledging that even internal clean-code efforts may still carry risk due to dependencies outside their immediate control (Company X CTO, 2025).

Research supports the severity of this risk. One recent study found that the fast-growing vector of supply chain attacks that target SMEs and their dependencies, has significantly increased, with open-source and third-party component vulnerabilities contributing to over 60% of successful software supply chain compromises in recent years (Ahmed & Abdullah 2024). Another study focusing on SMEs pointed out that supply chain risk factors such as "information security of suppliers" and "supplier reliability" have a strong negative effect on operational and financial performance (Kanyepe, Musasa & Wilbert 2025). A third article observed that "cyber threats in supply chains" are under-assessed by SMEs, leaving blind spots that attackers exploit (Konecka & Bentyn 2024). This aligns with Company X's situation: lean team, high dependency on external libraries/services, and limited internal capacity to continuously monitor all upstream risks.

Awareness of this issue by Company X's leadership does not negate the likelihood and impact it may have due to a compromised library or vendor tool that introduces malware or backdoor access could lead.

4.2.3.2 Treatment

To the existing methods for mitigating supply chain risk such as best practice methods and random risk assessments (Company X CTO 2025), the following are recommended to further increase company's ability to prevent such risk to occur in its environment.

Creating and maintaining a living Software Bill of Materials (SBOM), enables Company X to know exactly which open-source libraries and components are in use, assess their risk status, and respond quickly if vulnerability is discovered. As Ahmed & Abdullah (2024) points out, SBOMs are a key enabler for supply chain security and resilience. By integrating SBOM tracking into continuous integration pipelines and using vulnerability-scan tools, Company X can reduce both the likelihood and impact of a compromised component.

Integrating security earlier in the development lifecycle, especially focusing on third-party dependencies, container images, and supply-chain ingresses, is important. Konecka & Bentyn (2024) argue that SMEs often lack this proactive posture, which leads to hidden vulnerabilities and higher remediation costs. For Company X, this implies automated dependency checking runtime monitoring for anomalous behavior from third-party components, and periodic security audits of third-party libraries.

By combining these treatments to existing strategies, Company X will strengthen its resilience against software supply-chain threats, reducing both the probability of infiltration and the potential financial damage from a compromised chain.

4.2.4 Third-Party Service Outage or Provider Security Failure

4.2.4.1 Risk

Third party service dependencies introduce significant operational and financial risks, particularly for small IT companies like Company X, which rely heavily on cloud providers and external tools to run their core services. As a lean startup offering a SaaS solution, Company X's product is tightly integrated with third party Infrastructure that includes services for cloud computing, storage, authentication, and analytics. This operational model makes things run more smoothly, but it also makes things more dangerous if one of those providers goes down or is hacked. Company X CTO (2025) said during the interview that these kinds of dependencies are a "double edged sword" because they make things easier to scale but harder to control.

The Financial Stability Board (2019) notes that third party incidents can lead to large scale service disruptions and recommends increased oversight for cloud based operations. Wang, Li, Wang and Kang (2021) shows that how service correlation in cloud environments often amplifies the impact of a single failure. For SMEs, Nagahawatta, Warren, Salzman & Lokuge

(2024) explains that relying too much on external providers without having structured monitoring in place makes downtimes and delays in recovery more likely. They also point out that the consequences of these kinds of disruptions are bigger for small companies because they have limited in house IT redundancy and emergency response resources.

Because Company X has limited staffing and operates in a competitive B2B SaaS environment, third party outages pose not just an IT risk but a direct financial threat to business continuity. For this reason, this risk was selected for in depth analysis.

4.2.4.2 Treatment

Reliance on a single vendor for cloud infrastructure, identity management, or CI/CD tooling is a dangerous situation for small IT companies. As such Company X should implement adopt a modular or hybrid cloud architecture. According to Amajuoyi, Nwobodo and Adegbola (2024), multi cloud approaches significantly increase operational flexibility and reduce outage risk, especially for SMEs aiming to maintain service continuity and avoid vendor lock in. Adopting a modular or hybrid cloud architecture by using backup providers or maintaining the ability to rapidly migrate between services, when necessary, provides a solid treatment option.

Third party services should be evaluated with a structured risk scoring system. The criteria for scorings can be based on past incidents, data handling practices, geographic compliance such as GDPR and security certificates. As Kanyepe et al. (2025) point out, SMEs that implement strong vendor due diligence practices show lower rates of third party security incidents and better alignment with client expectations. Providers with higher scores should be selected for further use while those lacking transparency or documentation should be avoided or replaced if present.

4.2.5 Human Error & Social Engineering

4.2.5.1 Risk

Human error and social engineering remain two persistent global cybersecurity threats and Company X is no exception (Microsoft 2025). Although the small size of the team (5 10 employees) provide some bonus for internal visibility, due to the absence of formal security processes, the overall vulnerability to mistakes and manipulation is heightened. In the interview, Company X CTO emphasized that although phishing attempts and user mistakes have been largely manageable, the rise of AI powered phishing and attack tools could dramatically shift the landscape. He noted: “AI will soon automate phishing and attacks better than ever—we’re not yet prepared for that level” (Company X CTO 2025).

This concern is echoed by global trends. According to the Verizon’s 2025 Data Breach Investigations Report (2025), 60% of breaches involve a human element, including errors and social engineering. These attacks are becoming more difficult to detect due to advances in

generative AI, which can create new methods for manipulative action styles and personalize attacks. A study by OpenAI (2025) shows how AI enhanced phishing messages have a significantly higher success rate than traditional ones by showing examples. Study shows the attempted phishing methodologies to further advance awareness and the need for a more vigilant stance against possible human errors. Arween (2024) highlights that SMEs often underestimate the sophistication of modern social engineering techniques, especially those enhanced by artificial intelligence. These include voice spoofing, phishing email automation, and AI generated fake documents.

Financially, the consequences are significant. The IBM Cost of a Data Breach Report (2025, 6) notes that breaches involving social engineering or human error, which has the probability of 1 in 6, incur an average cost of $4.44 million, even in organizations with fewer than 100 employees. Company X's B2B SaaS business model where customer trust is central, the potential impact of a successful human-error or social engineering incident is high. Furthermore, because SMEs often lack incident detection and formal reporting structures, the likelihood of such attacks and impact in financial terms of this risk is high.

4.2.5.2 Treatment

Human error and social engineering is a permanent risk factor for every company. To effectively reduce the likelihood and impact of incidents caused by these risks, Company X can implement various methods to mitigate and manage this constant risk. These recommendations include awareness training and "no blame" reporting culture.

Company X should roll out regular, interactive training modules tailored for its context which is a small team, agile, SaaS environment company, focusing on phishing, impersonation, deep-fake content and AI-enhanced social engineering. Training modules should include realistic simulations of phishing attempts, especially those generated by AI tools, which Company X's CTO noted as an emerging threat vector. Free training resources such as Google's "Phishing Quiz" or the UK's "Cyber Essentials SME Training Portal" can help initiate the process with minimal cost. As Rombaldo Junior et al. (2023) states, technical training is a highly effective and low cost method that can exponentially increase readiness. He also states that improved cybersecurity literacy significantly enhances SME resilience. Ugbebor, Aina, Abass and Kushanu (2024, 386) mentions, contextual training reduced human-error incidents by 45-65% in SMEs.

Creating a workplace culture where employees feel safe to report errors or suspicious activity without feeling a negative emotion that can prevent reporting is vital for small teams. A "no blame" reporting policy can create an environment where early detection of possible issues and proactive mitigation are possible. Niroj (2025) indicates that SMEs which embed structured training and cultural awareness demonstrate improved security posture even with

minimal technical resources. This method points out the importance of combining procedural controls and behavioral design. Lastly, importing a two person verification method for critical operations such as production database exports, client data access further decreases Company X's risk exposure and create an additional layer of protection against both error and targeted social engineering.

By combining these two focused measures, Company X will significantly reduce both the likelihood and impact of human-error and social-engineering incidents. These measures are well-suited for a small IT company context. They require minimal infrastructure investment, leverage existing team structures, and directly target the "people risk" which literature shows is often the weakest link in SME cybersecurity frameworks.

4.2.6 GDPR or Regulatory Non-Compliance

4.2.6.1 Risk

For a small B2B SaaS provider like Company X, compliance with the GDPR and related regional legislation is not just a legal requirement, it is a vital business enabler. Company X processes sensitive personal data on behalf of worldwide clients, including enterprise users from countries with strict data residency and privacy expectations, such as Germany. As stated in the interview, regulatory compliance is an ongoing challenge: "Germany's interpretation of GDPR is much stricter... it creates pressure even when technically we're doing the right thing" (Company X CTO 2025).

The cost of failing to comply with the GDPR can result in administrative fines—up to €20 million or 4% of the company's annual global turnover (European Union 2016, Article 83). Moreover, non compliance risks reputational damage which as Company X CTO (2025) says in interview directly correlates with financial damage, contractual breaches, and loss of client trust. These possible consequences makes, also mentioned in the interview by Company X CTO "a reality, not a choice".

According to Tikkinen Piri, Rohunen & Markkula (2018), one of the primary challenges for SMEs under GDPR is the lack of formalized internal policies, poor documentation practices, and insufficient legal interpretation capabilities. These limitations expose startups like Company X to increased audit risks, especially when entering procurement contracts with larger organizations that demand demonstrable compliance processes. Compliance costs were higher during the early stages due to consulting needs and policy implementation for Company X and they have gone through internal audits which thanks to the strict approach by the leadership found no non compliance issues (Company X 2025).

Even with firm stance on staying in compliance by Company X, the risk emanating from unintended breaches and difficulty demonstrating accountability under Article 5 of the GDPR

persist. With new technologies and new methods appearing, so does the regulations for protecting data. Staying in compliance is a permanent risk that requires periodical attention.

4.2.6.2 Treatment

While Company X currently meets GDPR obligations, maintaining compliance over time requires constant attention. This need is especially heightened since Company X's business scales, adds features, and enters new markets. Following an organized method for GDPR regulations, Company X can prevent any risks that may occur when expanding. Compliance automation tools can help reduce manual workloads, flag deviations early, and ensure traceable audit trails. Tikkinen Piri et al. (2018) say that many small businesses have trouble with GDPR not when they first put it into place, but as their services change over time, when practices that used to be compliant may no longer be. Company X stays ahead of changes in the law and doesn't accidentally break the law by keeping an eye on things all the time. According to Ashraf (2021), small and medium sized businesses (SMEs) are getting more access to automated compliance management tools, which are a cheap and effective way to stay compliant. Company X could add this to their development pipeline, with alerts going off when the way they collect, process, or store data changes.

Transparency in cybersecurity measures taken is a critical factor in building trust for companies and this includes proactive client facing documentation, data protection summaries, and audit readiness reports (Amosh and Khatib 2024). This approach can serve both as competitive edge and as insurance against reputational damage in the event of a misunderstanding or incident. For Company X, this can be publishing GDPR compliance updates, issuing transparency reports, or providing clients with a compliance report during onboarding. These basic steps can reduce ambiguity and strengthen client trust in Company X.

4.2.7 Inadequate Incident Response Preparedness

4.2.7.1 Risk

Even though Company X completed ISO 27001 requirements and follows internal security measures, there is a constant concern about not being fully ready for cybersecurity incidents. The company's small size, having few employees and limited resources, make it difficult to maintain a state of readiness and check their preparedness regularly. According to interview, Company X CTO (2025) mentions their incident insurance provides some relief in financial side but also says "We've completed the ISO requirements… but still, one bad incident might cause big problems for us". The company has some policies and tools ready, but one single incident could be very serious.

This worry matches with wider industry wide concern about SME security maturity. Lots of small and medium sized businesses find it difficult to keep effective incident response skills

when facing real life challenges (Accountancy Europe 2022). Research shows that SMEs usually do not have enough detection tools, escalation workflows and learning steps after incidents. This can result in slower response and increased damage for the company (Arroyabe et al. 2024a). The need to grow development and client services often takes more importance than practicing simulations or spending on specialist incident response skills (Awan, Alam & Kamran 2025).

This is especially dangerous in a field like SaaS, where even brief disruptions or security issues can damage customer trust, break service agreements, or harm the company's reputation. If there isn't enough development in responding to incidents, it also makes investigating crimes, finding out why things went wrong and fixing them after difficult. This can cause the same weaknesses to happen repeatedly.

4.2.7.2 Treatment

For making Company X more resilient to security problems, it is good to use two main strategies. First, although Company X keeps incident response documents, it is important to do regular tabletop exercises and simulated breach scenarios. These practices help test and improve plans by creating fake real world attacks in a safe setting. They check how well employees know their jobs, escalation steps and communication methods during such incidents. Accountancy Europe (2022) suggests using lightweight but practical simulations as a cheap and effective method for SMEs to find unseen weaknesses in their incident response plans. These exercises can be done every three months with a small team, and the results can be recorded to show compliance and get ready for audits. This also strengthens employees' ability to make decisions and stay ready under stress, skills that are often ignored in plans that are only written (Awan, Alam & Kamran 2025).

Besides keeping ISO compliant documents, Company X should also have a simple playbook with step by step actions for various types like data breach, insider threat, SaaS provider outage. This playbook must include ready made communication messages for stakeholders, clients and regulators too. According to Arroyabe et al. (2024b), small and medium enterprises gain from using short, practical playbooks that match their real operations, staying away from long or too general guidelines. This method helps them react quicker and more uniformly when emergencies happen. Additionally, combining this playbook with a list of contacts and having a set spokesperson can lessen confusion and help keep a calm stance during emergencies.

Together, these treatments make Company X better prepared for incidents and ensure that even if a critical incident happens, the company can reduce disruption, keep its customers' information safe and quickly recover both operational and reputational integrity.

4.2.8 Loss of Customer Trust Following a Security Incident

4.2.8.1 Risk

SMEs are facing increased number of cyber attacks not because of negligence but because attackers are aware of the limited resources they have compared to larger corporations. As emphasized by Arroyabe et al. (2024a), cybercriminals increasingly target smaller firms since the growing digital footprint, dependency on SaaS infrastructure, and often limited incident response capacity are easier to attack vectors. Contrary to a common belief, being small a small company is not a deterrent for attackers, it is a dangerous idea that gives false confidence to SMEs which causes and increased risk exposure due to the assumption that "we’re too small to matter” (Rombaldo Junior et al. 2023).

Company X, despite being a vigilant and technically capable company, is no exception. During the interview and brainstorming session clearly pointed out overall stance of the company is security heavy. Both regulations and leaderships approach to the stance provides a solid defense against possible attacks. The company is also aware of a single incident can have a critical consequence (Company X CTO 2025; Company X 2025). Not just in the sense of the cost of the incident but rather the reputational effect of said incident is also a risk. As noted by Amosh and Khatib (2024), the reputational damage following a cyber incident can be more financially damaging than the technical fallout itself, especially for small vendors in highly competitive digital markets.

Therefore, Company X needs to recognize and be ready for the worst possible situations where trust is lost not just because of the breach itself, but also because of how it is managed. Losing customer trust was mentioned as one of the main financial risks for the company in both the interview and brainstorming session, not just something that could happen, but a real and serious concern.

4.2.8.2 Treatment

To rebuild trust after a security incident, Company X should focus on two important strategies that highlight clear communication, and focus repairing relationships. This is essential for recovery in a trust based SaaS environment. One of the best ways to regain client confidence is by being open and responsible when an breach happens. This means letting affected customers know quickly and share the recovery steps that have been taken to fix it. Amosh and Khatib (2024) found that small businesses that communicate openly regarding incidents and explain their technical response are more likely to keep their customers and even win new ones who value honesty. Company X can do this by setting up a formal process of informing stakeholders, customers and even employees for the scenario that includes personal emails, public updates on the status of the breach, and a specific person to reach

out to. The brainstorming session also stressed the importance of not waiting for the situation to become public and instead using transparency to stand out from competitors.

After a breach is contained, customers often want to know that “it won’t happen again”. Company X should create a structured process for communicating with clients that includes offering security assessment reports, explaining new security measures, and sharing summaries of audits or penetration tests. Arroyabe et al. (2024b) show that this kind of follow up strengthens long term trust, especially when customers see that the company is genuinely learning from the incident. Also, sharing security updates through customer newsletters can show that the company is constantly improving and helping users stay safe. Rombaldo Junior et al. (2023) suggest that SMEs should develop a playbook for assurance which includes sharing recovery timelines, reaching out to key clients proactively, and showing visible progress on promised improvements.

By using both approaches, Company X can turn a trust issue into a chance to show its strong commitment to data security and customer care.

4.3 Risk Evaluation

This matrix consolidates Company X’s cybersecurity-related financial risks identified in sections 4.2.1–4.2.8. Each row represents a distinct risk with:

- Impact scored on a 0–5 scale
- Likelihood on a 0–5 scale
- The risk value, calculated as $\text{Impact}^2 \times \text{Likelihood}$
- Root causes
- Expected consequences for the case company
- Existing treatment methods currently in place

Scores reflect interview insights, brainstorming outcomes, and the analysis presented earlier. Higher Risk Value indicates greater priority for mitigation and monitoring. The risk evaluation table will present the findings in Table 6 Risk Evaluation Calculation and Table 7 Risk Context & Controls in pages 35 37.

Risk	**Impact (0-5)**	**Likelihood (0-5)**	**Risk Value (Impact² × Likelihood)**
Data Breach / Data Leak	5	4	100
Cloud Misconfiguration & Infrastructure Failures	4	4	64
Software Supply Chain Vulnerabilities	4	3	48
Third-Party Service Outage / Provider Failure	3	3	27
Human Error & Social Engineering	3	3	27
GDPR or Regulatory Non-Compliance	4	2	32
Inadequate Incident Response Preparedness	4	3	48
Loss of Customer Trust Following Incident	5	2	50

Table 6 Risk Evaluation Calculation 2025

Risk	**Root causes**	**Consequences for the Company X**	**Existing treatment methods**
Data Breach / Data Leak	External attack, cloud or storage misconfiguration, insecure code or third-party dependencies, credential compromise	Severe legal, financial, and reputational damage, customer churn, contract termination	ISO 27001 information security management system, data processing agreements, data hosted in Germany and the European Union, encryption of recordings and transcripts, least-privilege access, code review and dependency checks, internal audits, cyber insurance
Cloud Misconfiguration & Infrastructure Failures	Untested configuration changes, weak monitoring, incorrect region selection or permissions, configuration drift	Service outage, data exposure, compliance findings, recovery costs	Reputable cloud providers, hosting in Germany and the European Union, role based access controls, logging and monitoring, risk review for significant changes
Software Supply Chain Vulnerabilities	Vulnerable open-source libraries, compromised third-party code, unvetted updates	Introduction of malware or backdoors, integrity loss, urgent patching, reputational harm	Dependency checks, code review within the software development lifecycle, tracked third-party components, periodic spot checks

Third-Party Service Outage / Provider Failure	Cloud or data center outage, upstream security incident, application programming interface vendor downtime, regional failure	Service disruption, service level agreement penalties, increased support workload, refunds or credits	Tier one providers, hosting and data residency in Germany and the European Union, status and availability monitoring, vendor risk review within the management system
Human Error & Social Engineering	Phishing, mistaken data sharing, procedural lapses, rushed operations	Account misuse, temporary exposure of data or access, internal disruption, recovery effort	Small team oversight, structured onboarding and offboarding, security awareness guidance, least-privilege access practices
GDPR or Regulatory Non-Compliance	Documentation gaps, evolving interpretations by clients or regulators, cross-border data handling issues	Regulatory fines, contract loss, reputational harm, additional audits	Data processing agreements, European Union jurisdiction, hosting in Germany, clear privacy policy, governance aligned with ISO 27001
Inadequate Incident Response Preparedness	Plans not rehearsed, reliance on a small number of key people, unclear escalation and communication	Slow containment, higher recovery cost, avoidable downtime, stakeholder confusion	Incident response plan, logging and monitoring, internal audits, cyber insurance, security ownership by the chief technology officer

Table 7 Risk Context & Controls 2025

5 Risk Treatment Proposals

The relevant treatment methods for identified risks are presented in their respective sections. Other present treatment methods are viable and can be adopted in parallel or at later stages, these five measures were selected. Proposals in this section can be implemented rapidly, require modest resources, and yield outsized reductions in both likelihood and impact across the highest value risks identified. In short, they are the easiest to implement well and provide the highest return. The proposals are in Table 8 Prioritized Proposals, page 38 39.

Proposal	**Reason**	**Importance**
Quarterly tabletop drills and one page communication playbook	Cuts decision time when minutes matter Exposes hidden gaps in roles and handoffs Reduces contradictory or delayed customer messages Builds confidence so people stay calm under pressure	Directly lowers impact for data breach and incident readiness Protects revenue by avoiding long outages and confusion Very low cost and uses people we already have Produces audit friendly evidence of preparedness
Cloud guardrails: misconfiguration alerts and monthly access clean ups	Misconfigurations are the fastest path to exposure Built in checks catch risky changes early Monthly access reviews shrink the blast radius Takes hours, not weeks, to set up and maintain	Tackles a high likelihood root cause with minimal effort Prevents both outages and accidental data exposure Improves compliance posture with little overhead Scales as the product grows without slowing teams

Dependency hygiene: simple component inventory and update alerts	Lets company answer “Are we affected?” immediately Reduces surprise from vulnerable third party code Automates most of the grunt work Keeps remediation cheap and routine instead	Targets a high impact, tricky to see risk Makes incident response faster and more credible Improves customer trust during security reviews Very low cost compared to the potential damage
Continuous awareness: short learning, monthly phishing practice, no blame reporting	Repetition changes behavior more than long, rare trainings Monthly practice keeps people alert to new tricks No blame culture speeds up self reporting Tailored content avoids wasting time	Reduces the most common entry path: people Improves early detection and limits spread Fits a small team’s schedule and budget Supports every other control we have
Customer trust pack: prepared messages and reassurance kit	Speeds transparent communication when it matters most Shows control and care, not panic Helps sales keep deals alive during a crisis Easy to maintain as a living set of documents	Directly addresses loss of trust risk after incidents Protects recurring revenue and renewals Differentiates us in competitive procurements Very low cost with high reputational payoff

Table 8 Prioritized Proposals 2025

6 Conclusion

The near and long term outlook for small information technology startups is difficult to predict and will likely present a shifting mix of threats and opportunities. For companies like Company X, the most consequential risks identified in this thesis center on data breach and data leak, cloud misconfiguration and infrastructure failures, software supply chain exposure, human error and social engineering, third party service disruption, regulatory noncompliance, and the loss of customer trust following an incident. Their relative importance can change quickly as technologies, attacker methods, customer expectations, and regulations evolve. The past few years have shown that major incidents can arise from both deliberate attacks and accidents, and that their financial effects on small firms can be critical. At the same time, advances in automation, artificial intelligence, and cloud services will continue to alter the operating environment, in positive and negative sense by creating both efficiencies and new categories of risk.

In such uncertainty, adaptability is the most reliable advantage. For a small, cloud based business, this means maintaining the ability to adjust controls, workflows, and supplier choices at short notice, all the while protecting core revenue through clear, timely communication with its customers. The practical proposals prioritized in this thesis such as quarterly incident tabletop drills with a one page communication playbook, enabling cloud guardrails with routine access reviews, a simple component inventory with automated update alerts, continuous awareness and no blame reporting, and a prepared customer trust pack, offers high return for modest cost and can be implemented with haste. Not every measure must be deployed at once. It is critical to also follow feasibility and the current risk picture. Above all, flexibility should guide Company X’s path. The biggest advantages of flexibility are staying lean enough to change direction quickly, reviewing risk and controls on a regular basis, and treating risk management as living processes rather than one time tasks. Risks rarely stay the same, and plans made are never permanent fixes or a final solution. The companies that thrive will be those that adapt and evolve both faster than the threats and with more clarity than their competitors.

References

Accountancy Europe. 2022. SME risk management – Cyber risks & resilience checklist. Accessed 10 November 2025. https://accountancyeurope.eu/wp content/uploads/2022/12/SME cyber security 2022_7.pdf?v1=&utm

Ahmed, A., & Abdullah, A. 2024. Enhancing Software Supply Chain Resilience: Strategy for Mitigating Software Supply Chain Security Risks and Ensuring Security Continuity in Development Lifecycle. International Journal on Soft Computing, 15(1/2). Article from arxiv. Accessed 10 November 2025. https://arxiv.org/abs/2407.13785

Amajuoyi, C., Nwobodo, L., & Adegbola, M. 2024. Transforming business scalability and operational flexibility with advanced cloud computing technologies. Computer Science & IT Research Journal, 5(6). 1469 1487. Article from ResearchGate. Accessed 10 November 2025. https://www.researchgate.net/publication/381717527_Transforming_business_scalability_and_operational_flexibility_with_advanced_cloud_computing_technologies

Amosh, H. & Khatib, S. 2024. Cybersecurity Transparency and Firm Success: Insights from the Australian Landscape. Australian Economic Papers 64(2). Article from Wiley. Accessed 10 November 2025. https://onlinelibrary.wiley.com/doi/10.1111/1467 8454.12385

Arroyabe, M., Arranaz, C., Arroyabe, I., & Arroyabe, J. 2024a. Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society, 78. Article from Science Direct. Accessed 10 November 2025. https://www.sciencedirect.com/science/article/pii/S0160791X24002185

Arroyabe, M., Arranaz, C., Arroyabe, I., & Arroyabe, J. 2024b. Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. Computers & Security, 141. Article from ScienceDirect. Accessed 10 November 2025. https://www.sciencedirect.com/science/article/pii/S0167404824001275?

Arween, F. 2024. Innovative Cybersecurity Awareness Programs in SMEs: Empowering Employee Behavior Against Social Engineering Threats. MSc. Computer and Systems Sciences. Stockholm University. Accessed 10 November 2025. https://www.diva portal.org/smash/get/diva2%3A1955683/FULLTEXT01.pdf

Ashraf, S. 2021. GDPR Implementation Framework for SMEs. MSc. Engineering Information Technology. Metropolia University of Applied Sciences. Accessed 10 November 2025. https://www.theseus.fi/bitstream/handle/10024/493722/Ashraf_Saira.pdf?sequence=2

Ashwood, P. 2023. The Common Cloud Misconfigurations That Lead to Cloud Data Breaches. CrowdStrike. Accessed 10 November 2025. https://www.crowdstrike.com/en us/blog/common cloud security misconfigurations/

Awan, M., Alam, A. & Kamran, M. 2025. Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review. Journal of Cyber Security and Risk Auditing, 2025(3). Article from theStap. Accessed 10 November 2025. https://jcsra.thestap.com/archives/volume 2025 3/68321de38e994a4fc1158063

Bowen, G. 2009. Document Analysis as a Qualitative Research Method. Qualitative Research Journal 9(2), 27 40. Article from ResearchGate. Accessed 10 November 2025. https://www.researchgate.net/publication/240807798_Document_Analysis_as_a_Qualitative_ Research_Method

Chaulagain, N. 2025. Developing Cybersecurity Awareness: A case study on Enhancing Employee Training in a Marine Manufacturing SME. BBA. BIT. Laurea University of Applied Sciences. Accessed 10 November 2025. https://www.theseus.fi/bitstream/handle/10024/894497/Chaulagain_Niroj.pdf?sequence=2

Cobos, V., & Cakir, S. 2024. A Review of the Economic Costs of Cyber Incidents. World Bank. Accessed 10 November 2025. https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee407 9180e81701969ad0a18.pdf?

Creswell, J. W. 2017. Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

ENISA. 2016. Guidelines for SMEs on the security of personal data processing. Accessed 10 November 2025. https://www.enisa.europa.eu/publications/guidelines for smes on the security of personal data processing

European Commission, 2020. User guide to the SME definition. Luxembourg: Publications Office of the European Union. Accessed 10 November 2025. https://single market economy.ec.europa.eu/publications/user guide sme definition_en

European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Accessed 10 November 2025. https://eur lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016R0679

Financial Stability Board. 2019. Third party dependencies in cloud services. Accessed 10 November 2025. https://www.fsb.org/uploads/P091219 2.pdf

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. 2008. Methods of data collection in qualitative research: Interviews and focus groups. British dental journal official journal of the British Dental Association. Article from ResearchGate. Accessed 10 November 2025. https://www.researchgate.net/publication/5495328_Methods_of_data_collection_in_qualitative_research_Interviews_and_focus_groups

IBM. 2025. Cost of a Data Breach Report 2025: The AI Oversight Gap. Accessed 10 November 2025. https://www.ibm.com/reports/data breach

ISO, 2018. ISO 31000:2018 Risk management – Guidelines. Geneva: International Organization for Standardization. Accessed 10 November 2025. https://www.iso.org/standard/65694.html

ISO, 2019. IEC 31010:2019 Risk management – Risk assessment techniques. Geneva: International Organization for Standardization. Accessed 10 November 2025. https://www.iso.org/standard/72140.html

ISO, 2022. ISO/IEC 27005:2022 Information security risk management. Geneva: International Organization for Standardization. Accessed 10 November 2025. https://www.iso.org/standard/80585.html

Kallio, H., Pietila, A M., Johnson, M., & Kangasniemi, M. 2016. Systematic methodological review: developing a framework for a qualitative semi structured interview guide. Journal of Advanced Nursing, 72(12), pp.2954–2965. Accessed 10 November 2025. https://onlinelibrary.wiley.com/doi/abs/10.1111/jan.13031

Kanyepe, James., Musasa, T., & Wilbert, M. 2025. Supply Chain Risk Factors, Technological Capabilities, and Firm Performance of Small to Medium Enterprises (SMEs). Journal of Small Business Strategy, 35(1). 115 128. Article from JSBS. Accessed 10 November 2025. https://jsbs.scholasticahq.com/article/125910 supply chain risk factors technological capabilities and firm performance of small to medium enterprises smes

Kolli, N. 2025. Navigating the Cloud: Security, Compliance and Risk Challenges in SME Adoption. Journal of Information Technology and Digital World, 7(3). 200 215. Accessed 10 November 2025. https://irojournals.com/itdw/article/view/7/3/1

Konecka, S., & Bentyn, Z. 2024. Cyberattacks as Threats in Supply Chains. European Research Studies Journal, 27(3). 778 796. Article from ERSJ. Accessed 10 November 2025. https://ersj.eu/journal/3467

LaMacchia, C., & Selznick, L. 2018. Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?. Journal of Business & Technology Law, 13(2). 217 253.

Article from Digital Commons@UM Carey Law. Accessed 10 November 2025. https://digitalcommons.law.umaryland.edu/

Microsoft. 2025. Microsoft Digital Defense Report 2025. Accessed 10 November 2025. https://www.microsoft.com/en us/corporate responsibility/cybersecurity/microsoft digital defense report 2025/

Nagahawatta, R., Warre, M., Slazman, S., & Lokuge, S. 2024. Towards an Understanding of Cloud Computing Adoption in SMEs. International Journal of Cyber Warfare and Terrorism, 14(1). Article from ScienceDirect. Accessed 10 November 2025. https://www.sciencedirect.com/org/science/article/pii/S1947343524000041

National Institute of Standards and Technology, 2025. Cybersecurity Risk. Accessed 10 November 2025. https://csrc.nist.gov/glossary/term/cybersecurity_risk

OpenAI. 2025. Disrupting malicious uses of AI: June 2025. Accessed 10 November 2025. https://cdn.openai.com/threat intelligence reports/5f73af09 a3a3 4a55 992e 069237681620/disrupting malicious uses of ai june 2025.pdf

Patel, D. 2015. Vendor Risk Management Demystified. ISACA Journal, 2015(4). Article from ISACA. Accessed 10 November 2025. https://www.isaca.org/resources/isaca journal/issues/2015/volume 4/vendor risk management demystified

Pickton, D., & Wright, S. 1998. What's SWOT in strategic analysis?. Strategic Change, 7(2). 101 109. Article from ResearchGate. Accessed 10 November 2025. https://www.researchgate.net/publication/246915222_What's_SWOT_in_strategic_analysis

Puyt, R., Lie, F., & Wilderom, C. 2023. The origins of SWOT analysis. Long Range Planning, 56. Article from ResearchGate. Accessed 10 November 2025. https://www.researchgate.net/publication/368734936_The_origins_of_SWOT_analysis

Rapley, J. 2025. Cloud Migration Security Risks for NZ SMEs. CyberOptic. Accessed 10 November 2025. https://www.cyberoptic.co.nz/post/cloud migration security risks for nz smes

Rombaldo Junior, C., Becker, I. & Johnson, S. 2023. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. arXiv preprint. Accessed 10 November 2025. https://arxiv.org/abs/2309.17186

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. 2020. Zero Trust Architecture. NIST Special Publication 800 207. Article from National Institute of Standards and Technology. Accessed 10 November 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800 207.pdf

Swot Analysis. 2013. E book. Team FME. Accessed 10 November 2025. https://talentandculture.wvu.edu/files/d/6ed4bddf 91fe 4f08 9904 c13b8b30cbe8/swot analysis tool.pdf

Tetteh, A. 2024. Cybersecurity needs for SMEs. Issues in Information Systems, 25, 235 246. Article from International Association for Computer Information Systems. Accessed 10 November 2025. https://iacis.org/iis/2024/1_iis_2024_235 246.pdf?utm

Tikkinen Piri, C., Rohunen, A. & Markkula, J. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. 34(1). 134–153. Article from ScienceDirect. Accessed 10 November 2025. https://www.sciencedirect.com/science/article/abs/pii/S0267364917301966?via%3Dihub

Tiusanen, R. 2018. Qualitative Risk Analysis. Handbook of Safety Principles.

Ugbebor, F., Aina, O., Abass, M. & Kushanu, D. 2024. Employee Cybersecurity Awareness Training Programs Customized for SME Contexts to Reduce Human-Error Related Security Incidents. Journal of Knowledge Learning and Science Technology, 3(3). 382-409. Article from JKLST. Accessed 10 November 2025. https://jklst.org/index.php/home/article/view/276

Vaideeswaran, N. 2025. What are Honeytokens?. CrowdStrike. Accessed 10 November 2025. https://www.crowdstrike.com/en us/cybersecurity 101/identity protection/honeytokens/

Verizon. 2025. 2025 Data Breach Investigations Report. Accessed 10 November 2025. https://www.verizon.com/business/resources/Tfea/reports/2025 dbir data breach investigations report.pdf

Wang, Y., Li, G., Wang, Z., & Kang, Y. 2021. Fast Outage Analysis of Large scale Production Clouds with Service Correlation Mining. Article from arXiv. Accessed 10 November 2025. https://arxiv.org/abs/2103.03649

Wilson, C. 2013. Brainstorming and Beyond: A User Centered Design Method. Waltham, MA: Morgan Kaufmann.

Interviews

- Company X CTO 2025

Brainstorming Workshop

- Company X 2025

ChatGPT has been used to edit the language of this text.

Figures

Tables