POLAR RISK

Cyber Risk Assessment Report

Example report

ACME B.V.

DATE	STATUS	CLASSIFICATION
16/10/2026	Draft	Confidential



Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Introduction

Between August and October 2026, Polar Risk carried out a Cyber Risk Assessment for ACME, a company specialised in metal processing, based in Amsterdam.

Background

In 2025, a ransomware attack disrupted operations at a similar metal processing company, bringing production to a halt for almost three weeks. At the same time, several of ACME's largest customers are subjected to the European Cyber Resilience Act and are tightening the cyber security requirements for their suppliers.

In light of these developments, ACME's board raised the following questions about their cyber security:

1. Could a cyber incident bring ACME's production to a standstill?
2. Where does ACME stand in terms of cyber security?
3. How large is the cyber risk for ACME?
4. What can ACME do with or about this risk?

Polar Risk was asked to conduct a Cyber Risk Assessment and provide an evidence-based answer to these questions, including clear insight into ACME's cyber risk exposure and recommendations for addressing it.

Cyber Risk Assessment

The Cyber Risk Assessment answers three central questions, which together address the board's questions:

1. What are the most relevant cyber risks?
2. How large are these cyber risks in euros?
3. How safe is safe enough?

The results are based on interviews with stakeholders from across the organisation, including the IT Manager, the CISO, the HR Manager and the Head of Finance. Combined with Polar Risk's market and sector data, these insights provide a sound picture of ACME's cyber risk.

Should this report give rise to any questions, or should further explanation be required, please do not hesitate to contact us.

Polar Risk's general terms and conditions apply to this Cyber Risk Assessment. This report is intended solely for ACME B.V. and for the purpose for which it was prepared. No rights can be derived from this report by third parties.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Contents

#	CHAPTER	PAGE
1	**Management summary** A high-level summary of the outcomes of the Cyber Risk Assessment and the answers to the board's questions.	4
2	**Organisation profile** The organisational context that makes ACME's cyber risks unique.	6
3	**Cyber risks** The cyber risks identified for ACME, worked out and financially substantiated within ACME's context.	9
4	**Safe enough** An assessment of the extent to which ACME can and is willing to bear its cyber risks (financially).	18
5	**Conclusion & advice** Concluding advice that answers the three central questions of the Cyber Risk Assessment and the board's questions, with options for dealing with the cyber risk.	21

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Management summary

Cyber risk

ACME depends heavily on IT and OT for its production. Production planning, order processing and logistics run on SAP S/4HANA, and Siemens OT systems control the production lines. If these systems are disrupted, production comes to a standstill almost immediately and deliveries to customers are delayed.

For ACME, the financial impact of cyber incidents therefore lies mainly in lost revenue due to production standstill, contractual penalties for late delivery and the costs of recovery.

An overview of ACME's cyber risks is shown on the next page.

Safe enough

Whether and how ACME deals with its cyber risks depends on two questions:

- *How much risk is ACME willing to take? (**risk appetite**)*
- *How much risk could ACME bear in the worst case without getting into financial difficulty? (**risk capacity**)*

The risk appetite has been set at **€500,000** and the risk capacity at **€6,350,000**.

The analysis shows that two cyber risks, ransomware and a cloud provider disruption, largely exceed the risk appetite. A data breach exceeds it only in the worst case. All cyber risks remain below the risk capacity.

Current situation and next steps

ACME has a solid foundation for information security, with policies, processes and technical measures that suit its position in the manufacturing industry. However, these measures have not been implemented consistently everywhere, detection capability is limited and there is insufficient insight into dependencies within the supply chain.

Polar Risk sees the following priorities for mitigating the cyber risk:

1. Tightening access rights and introducing phishing-resistant MFA for critical systems.
2. Testing back-ups and recovery procedures, and enforcing segmentation between IT and OT.
3. Mapping critical suppliers and agreeing continuity arrangements with them.

In summary, Polar Risk advises the following on ACME's cyber risks:

#	RISK	NEXT STEP
1	Data breach	✓ Accept
2	Ransomware	↘ **Mitigate**
3	Cloud provider disruption	↘ **Mitigate**

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Management summary



The chart above visualises the financial impact of each identified cyber risk, should it occur.

The financial impact of a cyber risk is a range consisting of the minimum impact, the maximum impact and the impact that 50% of cases fall below or above (most likely).

Minimum Most likely Maximum

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

2

Organisation profile

The nuances that make ACME’s cyber risks unique

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Organisation profile

Business operations

ACME is a metal processing company in Amsterdam that manufactures complex steel products to customer specification. It employs 250 people, most of whom work on site. Because its work is highly specialised, ACME has few competitors: two in the Netherlands and at most fifty across Europe.

Revenue

ACME's revenue in 2025 was **€55,000,000**, from three streams:

1. **Dutch market** (65%): €35,750,000
2. **European market** (30%): €16,500,000
3. **Design support and other** (5%): €2,750,000

Market and objectives

All sales markets are within the European Economic Area (EEA), and ACME is a vital link in its customers' supply chains. ACME aims to grow revenue by 10% over the next five years through:

- More orders for ultra-complex, higher-margin steel products.
- A larger customer base in the Benelux.

Laws and regulations

ACME is subject to Dutch law. Specifically relevant to cyber risk are:

- The GDPR, supervised by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).
- Customer contracts on confidentiality, delivery times and penalty clauses.

IT and data

ACME's IT landscape is hybrid: traditional on-premise systems are combined with modern cloud solutions. IT and OT are increasingly integrated, enabling efficient production and real-time monitoring.

On-premise

In the production environment, OT systems such as Siemens WinCC and Siemens S7 control the physical processes. Segmentation between the IT and OT networks is in place, but not strictly enforced. Identity and access management is based on an on-premise Active Directory combined with Microsoft Entra ID.

Cloud and other IT services

The core of the business is supported by the ERP system SAP S/4HANA, which handles production planning, order processing and logistics. This environment is hosted by an external cloud provider. ACME uses Microsoft 365 for e-mail, file storage and collaboration.

In some cases, suppliers have remote access to systems, for example for maintenance. The authorisations for this access are not always set up consistently or securely.

ACME has a small internal IT team led by the IT Manager. An external managed service provider supports network and workplace management.

Future developments

ACME plans to modernise parts of its IT landscape, including partial cloud migration and further digital integration of the production environment. This offers efficiency and scalability, but also enlarges the attack surface.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Organisation profile – continued

Data

ACME's data consists mainly of production data, customer information and intellectual property, such as technical designs, drawings and product specifications. Much of this information is provided by customers under strict confidentiality agreements.

Like any employer, ACME processes personal data: of 250 current and around 400 former employees, and the contact details of some 1,500 contacts at customers and suppliers. HR files may contain special categories of personal data, such as sickness records.

Threats in the industry

The manufacturing industry is a popular target for cybercriminals, because a production standstill almost always leads to lost revenue. This makes the industry susceptible to extortion through ransomware or DDoS attacks, as the ransomware attack on Norsk Hydro in 2019 showed.

Manufacturers such as ACME produce specialist steel products to customer specification, from custom screws to complex parts for semiconductor machines. This puts the industry in the sights of state-sponsored attackers interested in specifications and blueprints.

On a positive note, the industry has many family businesses with close-knit workforces. Incidents deliberately caused by employees are below average.

Cyber security

ACME has a mature foundation, with policies, processes and technical measures in place, such as back-ups, endpoint protection, MFA for remote access and administrator accounts, and logging and monitoring of critical systems. Roles for incident response have been assigned.

Previous incidents

In 2025, a phishing e-mail led to a compromised Microsoft 365 account. The account was blocked within a day and no evidence of data exfiltration was found.

Points of attention

Despite this solid foundation, a number of points require attention:

1. Detection capability is limited, especially in the OT environment and for data flows in the cloud. Attackers may go unnoticed for longer.
2. Access rights are broad and their use is poorly monitored. Users can access more systems, production data and designs than strictly necessary.
3. Segmentation between IT and OT is not strictly enforced, so attackers could move from IT to OT.
4. Back-ups are made, but recovery procedures have only been tested to a limited extent.
5. Insight into dependencies on suppliers is still developing. Continuity plans have not been tested jointly with suppliers.

The conclusion and advice discuss follow-up actions in more detail.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

3

Cyber risks

Relevant cyber risks worked out for ACME and substantiated with likelihood and financial impact

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

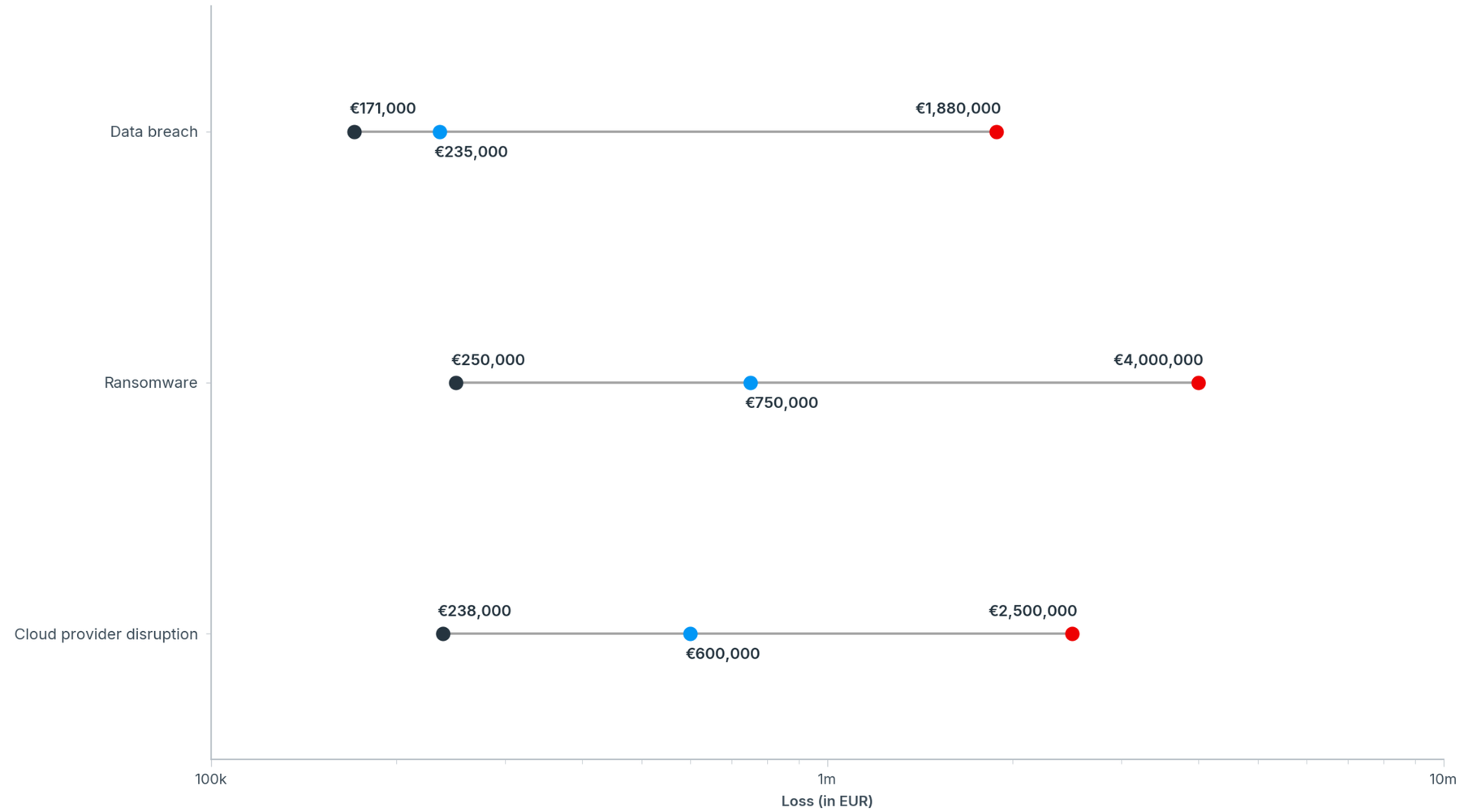
Financial impact of cyber risks

The chart below visualises the financial impact of each identified cyber risk, should it occur.

The financial impact of a cyber risk is not a fixed figure, but a range consisting of the lowest possible impact (minimum), the highest possible impact (maximum) and the impact that 50% of cases fall below or above (most likely).

In this chart, the range of the impact is visualised with three dots:

Minimum Most likely Maximum



Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

1 Data breach

RISK SCENARIO

Cybercriminals use a compromised employee account to steal personal data and confidential customer designs from ACME's systems.

SCENARIO EXPLAINED

Spear phishing, misuse of compromised accounts and poorly secured collaboration platforms are the most likely attack routes, supplemented by risks from insiders and third parties with access.

Specific detection of unusual data flows is lacking. As a result, data exfiltration via legitimate accounts or the cloud can go unnoticed for a long time.

LIKELIHOOD

Best case	Typical case	Worst case
Once every ±12 years	**Once every ±8 years**	**Once every 5 years**
(8% per year)	(12% per year)	(20% per year)

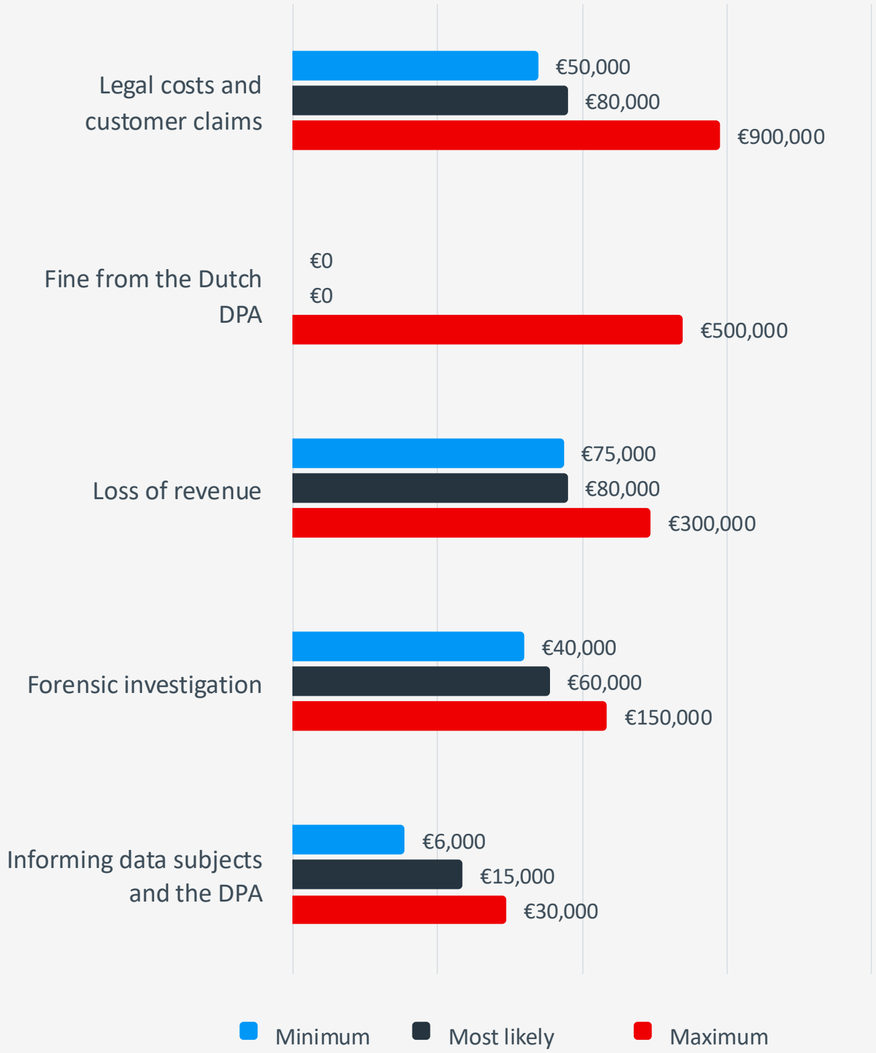
FINANCIAL IMPACT



Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

1 Data breach

WHAT DRIVES THE FINANCIAL IMPACT?



COST ITEMS EXPLAINED

The largest cost item is the leak of confidential customer information. Customers can claim damages under confidentiality agreements, which also leads to legal costs.

A breach of confidentiality can also cost ACME orders: some customers may (temporarily) move work to a competitor.

From a technical point of view, a forensic investigation is needed to establish how the breach occurred and which data was stolen.

Affected employees and contacts must be informed and the breach reported to the Dutch Data Protection Authority, which may impose a fine.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

2 Ransomware

RISK SCENARIO

Cybercriminals gain access via phishing or a supplier's remote access and deploy ransomware. Encryption of IT and OT systems brings production and deliveries to a standstill.

LIKELIHOOD

Best case	Typical case	Worst case
Once every 10 years	**Once every ±7 years**	**Once every ±3 years**
(10% per year)	(15% per year)	(30% per year)

SCENARIO EXPLAINED

Before encrypting systems, cybercriminals usually also steal data and threaten to publish it.

Phishing and vulnerabilities in external access (such as Citrix) are the most realistic entry points, based on incident data from comparable organisations.

Limited detection and weak segmentation between IT and OT allow attackers to reach the production environment before they are stopped.

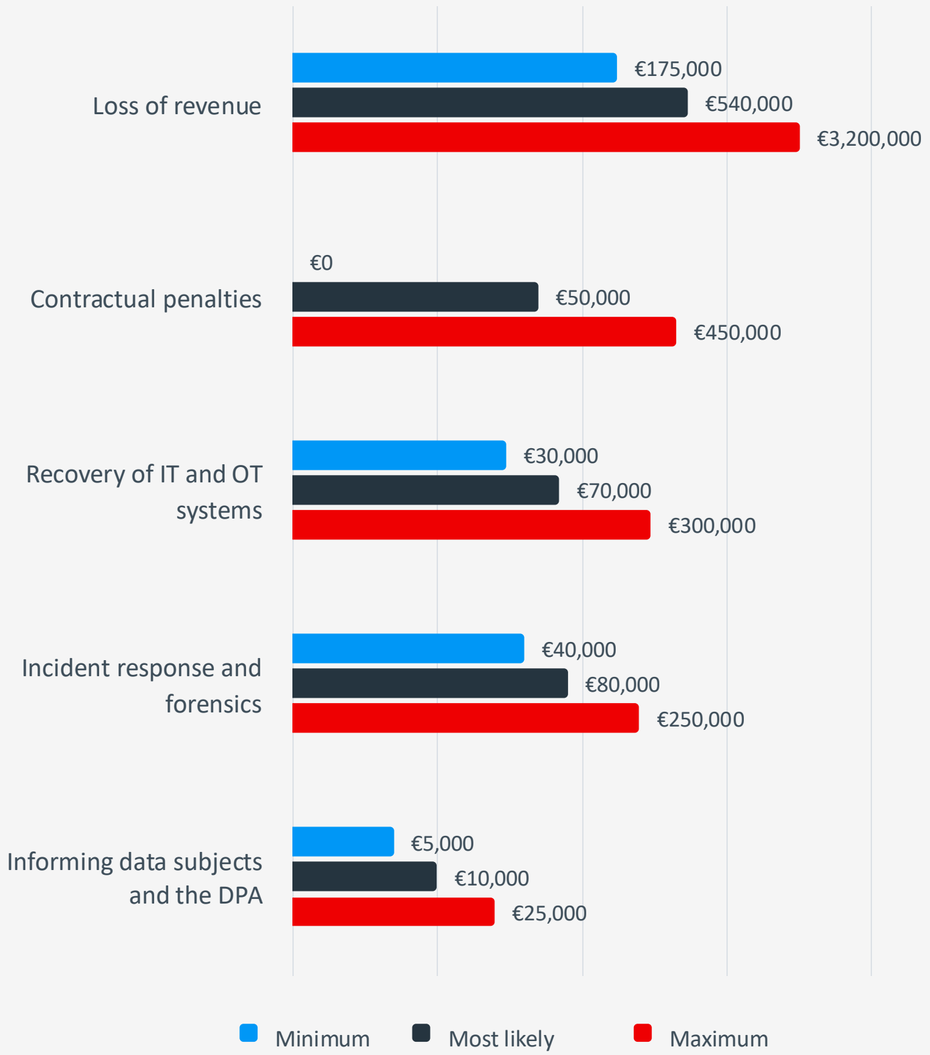
FINANCIAL IMPACT



Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

2 Ransomware

WHAT DRIVES THE FINANCIAL IMPACT?



COST ITEMS EXPLAINED

The potential losses are mainly driven by lost revenue due to production standstill. Without production planning and control systems, production comes to a halt within hours.

Back-ups are available, but recovery procedures have only been tested to a limited extent. This lengthens recovery time and increases costs, for example for forensic investigation and external specialists.

Late deliveries can lead to contractual penalties from customers.

As data is usually stolen as well, data subjects must be informed and the breach reported to the Dutch DPA.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

3 Cloud provider disruption

RISK SCENARIO

An outage at the cloud provider that hosts SAP S/4HANA makes ACME's ERP environment unavailable, disrupting production planning and deliveries.

LIKELIHOOD

Best case	Typical case	Worst case
Once every 10 years	**Once every ±8 years**	**Once every ±7 years**
(10% per year)	(12% per year)	(15% per year)

SCENARIO EXPLAINED

Technical failures, cyber incidents and dependencies on underlying cloud or network providers are the most realistic causes of an outage, based on incidents at comparable organisations.

ACME lacks full insight into the availability and performance of its external IT providers. Fallback options are limited and continuity plans have not been tested jointly with the provider.

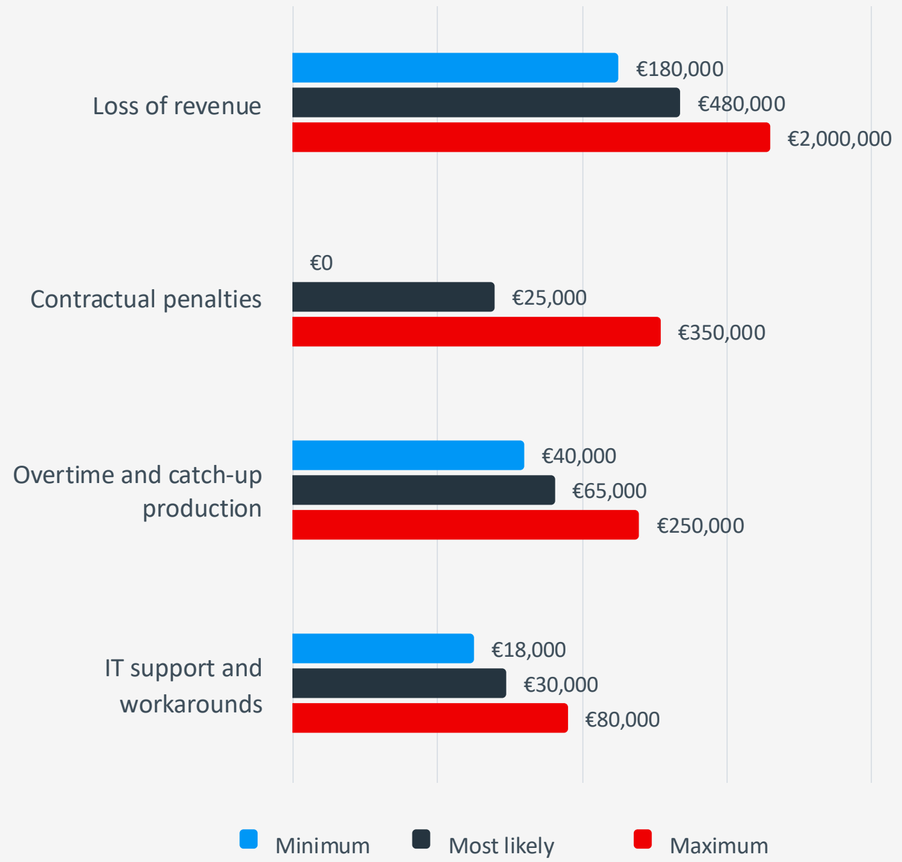
FINANCIAL IMPACT



Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

3 Cloud provider disruption

WHAT DRIVES THE FINANCIAL IMPACT?



COST ITEMS EXPLAINED

An outage of SAP S/4HANA directly disrupts production planning, order processing and logistics. Production can continue for a short time on existing work orders, after which output falls sharply.

Part of the lost production can be made up with overtime, at additional cost. If deliveries are late, customers may impose contractual penalties.

Internal IT staff and external specialists spend time on workarounds and recovery, such as manual order processing.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Prioritised overview of cyber risks

#	RISK	ANNUAL RISK (P90)	FINANCIAL IMPACT
1	Ransomware	€656,676	€0 – €4,167,694
2	Cloud provider disruption	€403,971	€0 – €2,486,936
3	Data breach	€208,992	€0 – €1,728,040

Cyber risks vary widely in frequency and impact. They range from common risks with limited consequences to rare risks with severe consequences. To compare these different risks effectively, Polar Risk prioritises cyber risks on the basis of the annual risk.

The likelihood and financial impact of each cyber risk are converted to a calendar year, so that cyber risks can be compared with one another. The specific data point used for this is the P90: in 90% of all simulated years, the annual loss is this amount or lower.

For ACME, the prioritisation based on annual risk matches that of the financial impact. Ransomware stands out, combining the highest likelihood with the highest impact. A cloud provider disruption is less likely, but its most likely impact (€600,000) is well above that of a data breach (€235,000).

Note: the annual risk says nothing about which risks will occur, or with what impact. It is purely a comparison tool that prevents rare cyber risks from claiming all the attention because of their high impact.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

4

Safe enough

Insight into which cyber risks ACME can and is willing to bear

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Risk appetite and risk capacity

Whether ACME is safe enough depends on the risk the organisation can and is willing to bear. Organisations do not take risks without reason; they do so because taking risks creates value.

With cyber risks, this usually means that using IT and holding and processing data helps the organisation achieve its objectives. For ACME, these are:

1. Reliably manufacturing complex steel products to customer specification, on time and to the agreed quality.
2. Growing revenue by 10% over the next five years through more orders for ultra-complex steel products.
3. Expanding the customer base in the Benelux.

For ACME, the question is therefore twofold:

- How much risk is ACME willing to bear to achieve these objectives?
- How much risk can ACME bear financially?

Risk appetite

Interviews with stakeholders show that ACME considers an annual loss of around €500,000 to be the maximum acceptable. This means that ACME is willing to accept this amount each year as the direct cost of cyber incidents in order to achieve objectives 1 to 3.

In practice, this does not mean that €500,000 in additional costs will be incurred every year. Part of the impact consists of costs the organisation would incur anyway, such as the hours employees spend resolving an incident.

Risk capacity

The 2025 annual report shows that ACME has €6,350,000 in liquid assets.

In the worst case, ACME could bear up to €6,350,000 in risk for the coming year without running into problems with payment obligations or other solvency issues.

This does not automatically mean that it is desirable to take €6,350,000 in risk.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Bearable and unbearable cyber risk



Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

5

Conclusion & advice

The way forward

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Advice

Based on the cyber risks relevant to ACME and the established risk appetite and risk capacity, Polar Risk advises ACME to take the following next steps:

#	RISK	NEXT STEP	EXPLANATION
1	Data breach	✓ Accept	Risk largely below risk appetite
2	Ransomware	↘ **Mitigate**	Detection, segmentation and recovery
3	Cloud provider disruption	↘ **Mitigate**	Redundancy and supplier management

Organisations can broadly do four things with cyber risks:

1

Accept the risk

The organisation acknowledges that the risk exists, but takes no further measures to reduce its likelihood or impact.

2

Mitigate the risk

The organisation takes measures to reduce the likelihood and/or impact.

3

Insure the risk

The organisation takes no measures to reduce the likelihood and/or impact, but transfers the financial impact to an insurer in return for a premium.

4

Avoid the risk

The IT system, data or business activity that causes the risk is avoided. This often means switching off a system, no longer offering a product or service, or no longer serving a particular market.

Introduction
Summary
Organisation profile
Cyber risks
Safe enough
Conclusion & advice

Conclusion

ACME has a solid foundation for cyber security, suited to its role as a specialist player in the manufacturing industry. At the same time, variations in implementation, limited detection capability and dependence on external parties mean that both the likelihood of incidents and their potential impact are elevated.

In particular, the combination of limited visibility of malicious activity, broad access rights and dependence on suppliers means that incidents are not only more likely, but can also escalate more quickly into disruptions that directly affect production, delivery reliability and revenue.

For an organisation like ACME, which is a critical link in its customers' supply chains, cyber risks can feed directly through to customers and contractual obligations.

Two of the three cyber risks identified, ransomware and a cloud provider disruption, exceed ACME's risk appetite. A data breach exceeds it only in the worst case. All three risks remain below the risk capacity.

The further development of the IT landscape, including increasing cloud adoption, closer integration of IT and OT and more digital supply chain links, will enlarge the attack surface and increase dependence on external parties. This calls for a more proactive approach to cyber security that builds resilience structurally.

It is up to ACME to decide whether or not to act on these cyber risks. Polar Risk sees opportunities to combine the planned modernisation of the IT landscape with addressing them.

Polar Risk's main recommendations:

- Tightening access rights and introducing MFA for critical accounts.
- Strengthening detection and response, including in the OT environment.
- Enforcing network segmentation between IT and OT.
- Setting up Business Continuity Management and IT Disaster Recovery, and testing recovery regularly.
- Reducing dependence on a single cloud provider and setting up third-party risk management.



POLAR RISK