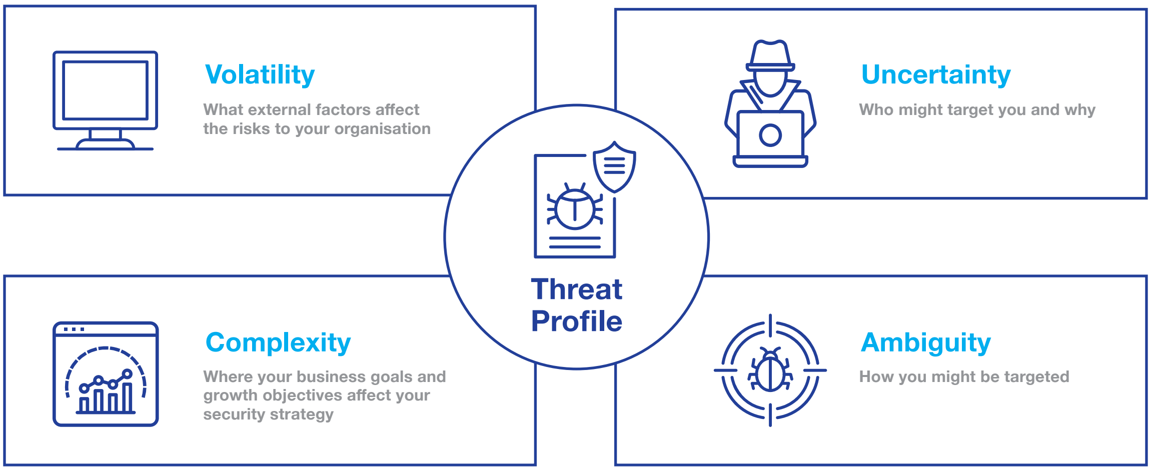
Your company in the conflict area of digitalisation and IT security



Volatility

What external factors affect the risks to your organisation

Uncertainty

Who might target you and why

Threat Profile

Complexity

Where your business goals and growth objectives affect your security strategy

Ambiguity

How you might be targeted

VUCA – The challenges in a digitalised world

The term VUCA summarises the challenges that companies have to face in an increasingly digitalised world. Digitalisation and thus the development towards industry 4.0 present business and society with new challenges. Because new technologies are being developed faster and faster, the threat level for companies is constantly changing. VUCA is an acronym for the English terms ‚volatility‘, ‚uncertainty‘, ‚complexity‘ and ‚ambiguity‘.

You can use the following checklist to check how your company is positioned in the conflict area of digitalisation and security.

Volatility –
What external factors influence the risk your business has of being attacked:

- Trickle-down effect: Is your team ready to protect itself against tools used by government-sponsored groups?
- Zero days: Which protocols do you use if an unknown weakness appears in your software, hardware or firmware?
- Supply chain: How do you check your suppliers?

Uncertainty –
Who can make you a target and why?

- What valuable assets (invoices, IP assets, M&A data or personal information about your customers) are available to your company that could be exploited by attackers?
- Who counts you among their suppliers?

Complexity –
To what extent does your strategy and growth plan affect your IT security?

- Digital transformation increases your attack radius - is this continuously monitored and who has taken over these tasks?
- How do you deal with updates and upgrades in your company?
- Can data relevant to business be compromised? And how do you behave when you are forced to go offline?

Ambiguity –
How you can be attacked:

- Pishing and social engineering
- In-memory attacks that are continuously being developed
- Malicious file attachments

Source: https://www.f-secure.com/content/dam/f-secure/en/business/countercept/collaterals/digital/f-secure-countercept-rethinking-response-whitepaper.pdf

Take on the path of digitalisation safely with AXSOS

Regarding AI
61% of companies with a digitalisation strategy use AI to identify business opportunities that they would otherwise have missed. 77% of CEOs say that AI has the potential to increase weaknesses and disruptions in their own business model.

Regarding cloud
By 2021, 94% of data is to be processed via cloud platforms.

66% of IT executives say security is their greatest concern when it comes to cloud platforms.

Regarding IoT
78% of decision makers believe that their company is very likely to be exposed to data loss or theft due to IoT.

48% of companies using IoT technologies have no processes in place if devices are hacked.

Attackers and their motivation

» Groups commissioned by states/nations: These groups steal, blackmail or secretly enter networks to monitor company processes and to view potentially valuable data. These attackers don‘t give up until they have reached their goal.

» Organised criminal groups: Their greatest motivation is money. Their business: Direct data theft or invoicing fraud. While groups commissioned by states steal for their respective clients, the aim of these groups is to resell data.

» Cyber criminals: They cause damage or publish information inside or outside a company - for both financial benefits and personal political motives.

» Script kids & hack activists: Cause damage simply because they can!

Valuable investments in your company:

» Their goal is to compromise your supply chain. Even if your company has no valuable assets, one of your customers to whom you provide services could be the target of an attack. Attackers also aim to compromise supply chains.

» Their goal is invoicing fraud. Every company issues invoices - in this case, the attackers secure rights to be able to access invoices, to change them or to create them with changed data. In most cases, no one notices that an invoice was created at all.

» Their goal is to resell personal information. If you have saved personal data (name, birthday or bank details), you can become the target of attackers who are aiming to resell these data or compromise your internal data. This is what you are fighting against. You have to be prepared for this.

Attackers have more time than goals:
They plan their actions over months by testing how email filters work, which employees are susceptible to social engineering tactics, and by checking firewalls for weaknesses.

Attackers only need one direct hit:
Attackers only need one direct hit. Those defending, on the other hand, must be successful in all their actions and, at best, must always be one step ahead.