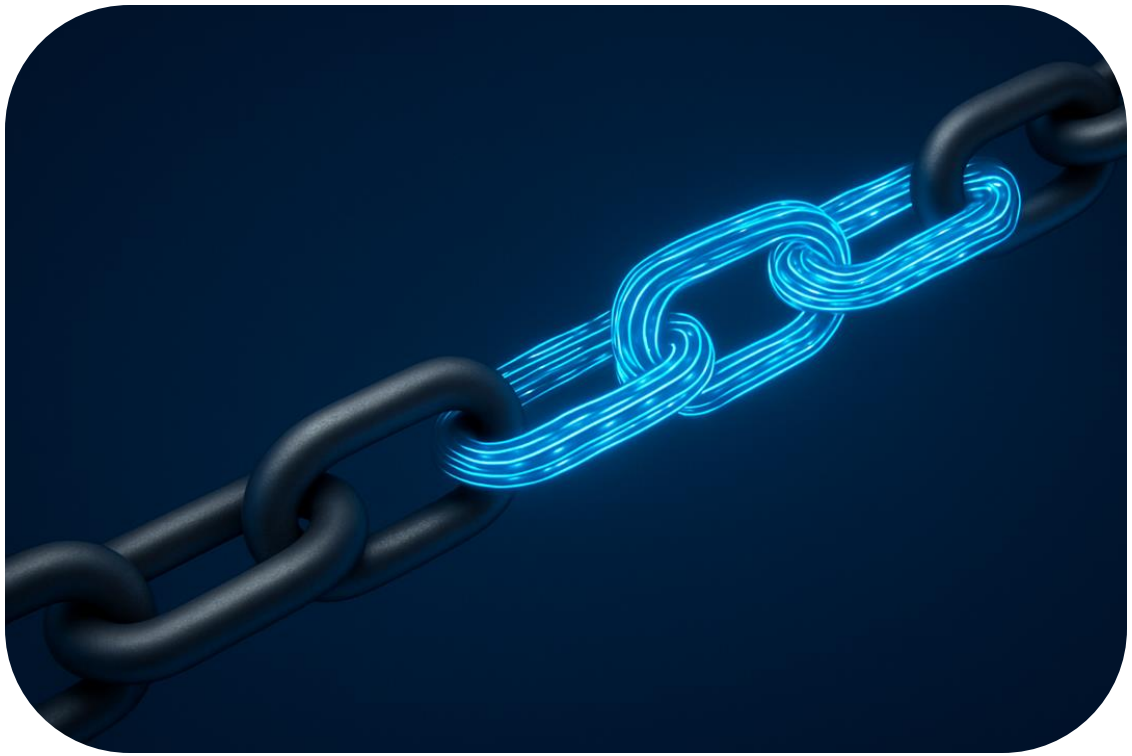
Supply Chain Resilience and Cybersecurity



Welcome

Supply chain resilience & cybersecurity

“When the interconnected nature of our supply chain is commonly built on misplaced trust and wrong assumptions; What can go wrong?”

By Roy Coppieters & Yorben De Maeyer
Director & Senior Manager crisis leadership & resilience PwC Belgium

Grant me the strength to accept the things I cannot change, the courage to change the things I can, and the wisdom to know the difference between them.

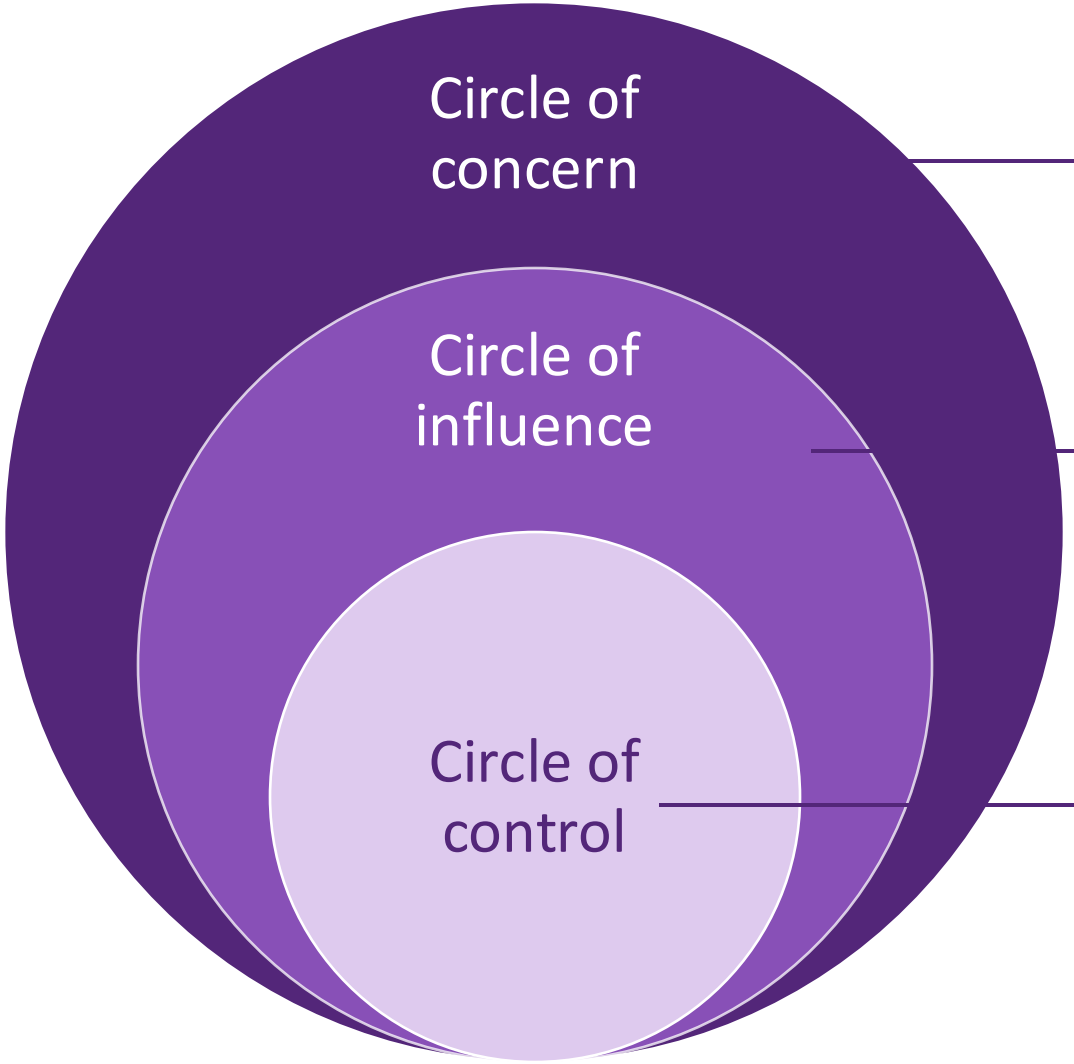
What we want to impart to you today:

Insights into ‘cyber’ as a primary risk for supply chains

Awareness of the impact of disruption through real cases

Practical examples and tips to increase supply chain resilience

Is all under your literal control? To assume is to make an…



Wide range of concerns of which we have **no control** over the outcome. *E.g. Geopolitics*

The concerns we can do something about. We do not have control over the outcome, but **can influence it with what we are able to control**. *E.g. preparedness of suppliers*

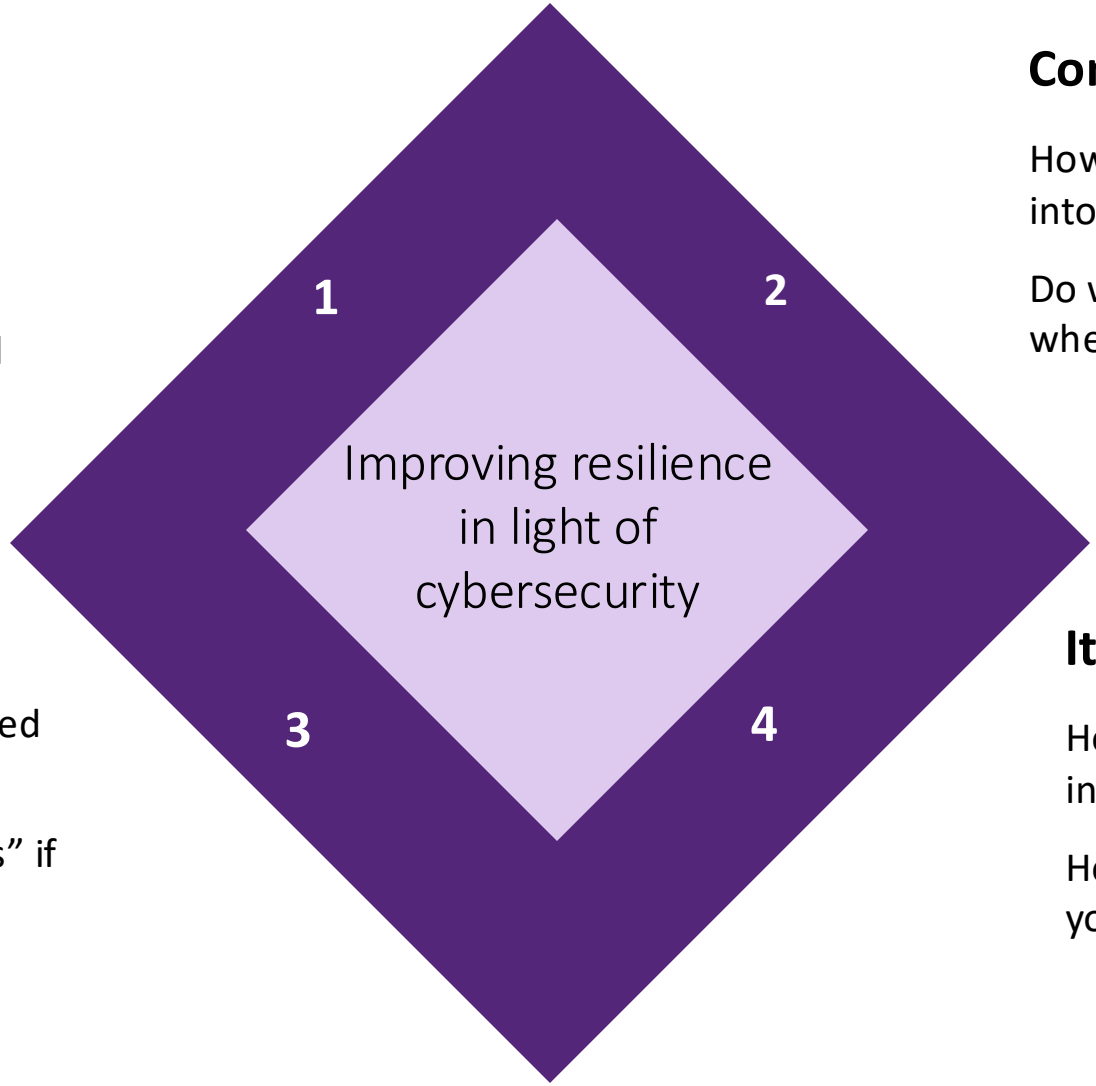
What we can **directly control** or impact through our thoughts, words and actions. *E.g. our internal cybersecurity posture and controls*

Navigating pitfalls to successfully address challenges

Control

What is the importance of understanding where your technology resides?

How can you better secure your digital assets that support your supply chain?



Concern

How do we translate big picture stuff into concrete risks and impacts?

Do we have alternatives in place for when the worst comes to pass?

Influence

What are the consequences of increased outsourcing for our supply chain?

How reliable is “the hand that feeds us” if it is starving itself?

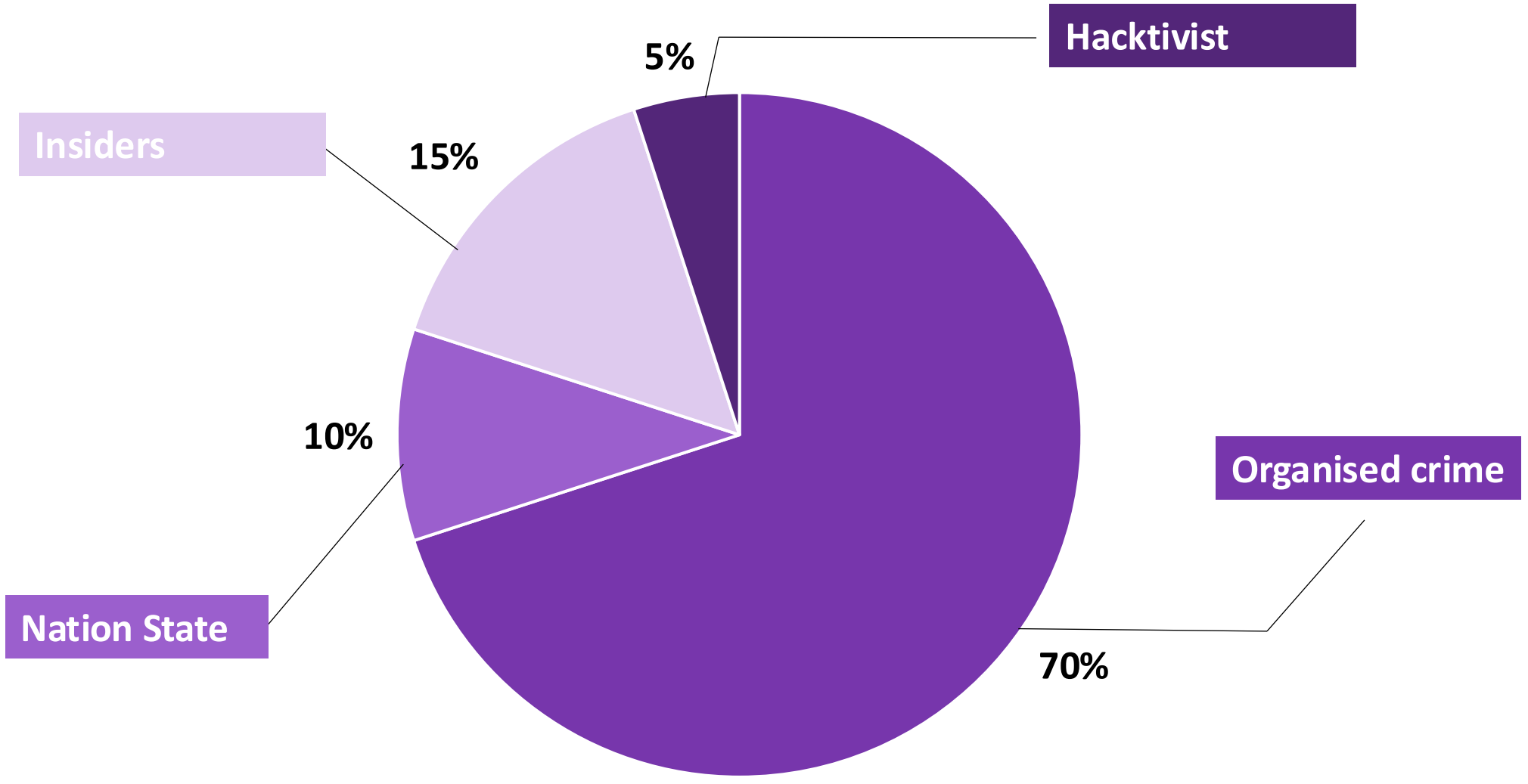
It’s about people

How does a cyber impact translate into a people impact?

How do you protect your people and your reputation?

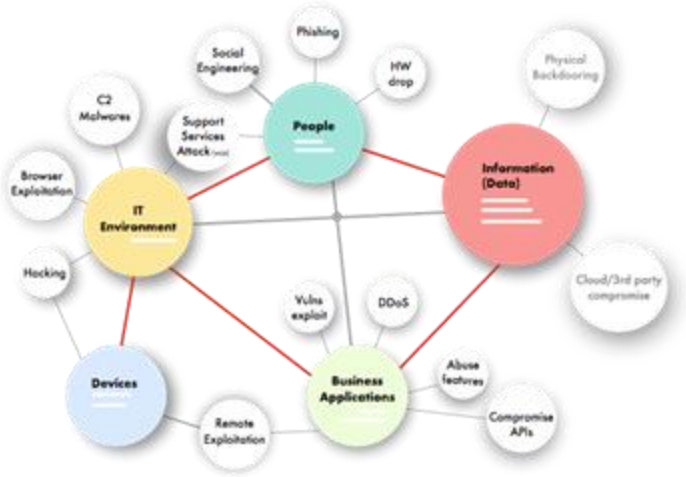

Your adversary

Who are the threat actors?



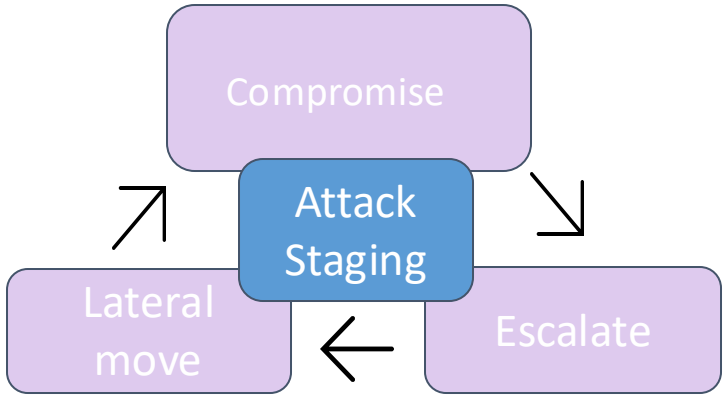
Understanding the cyber killchain

1 Attack



Pick one or multiple
Breach Vectors

2 Compromise



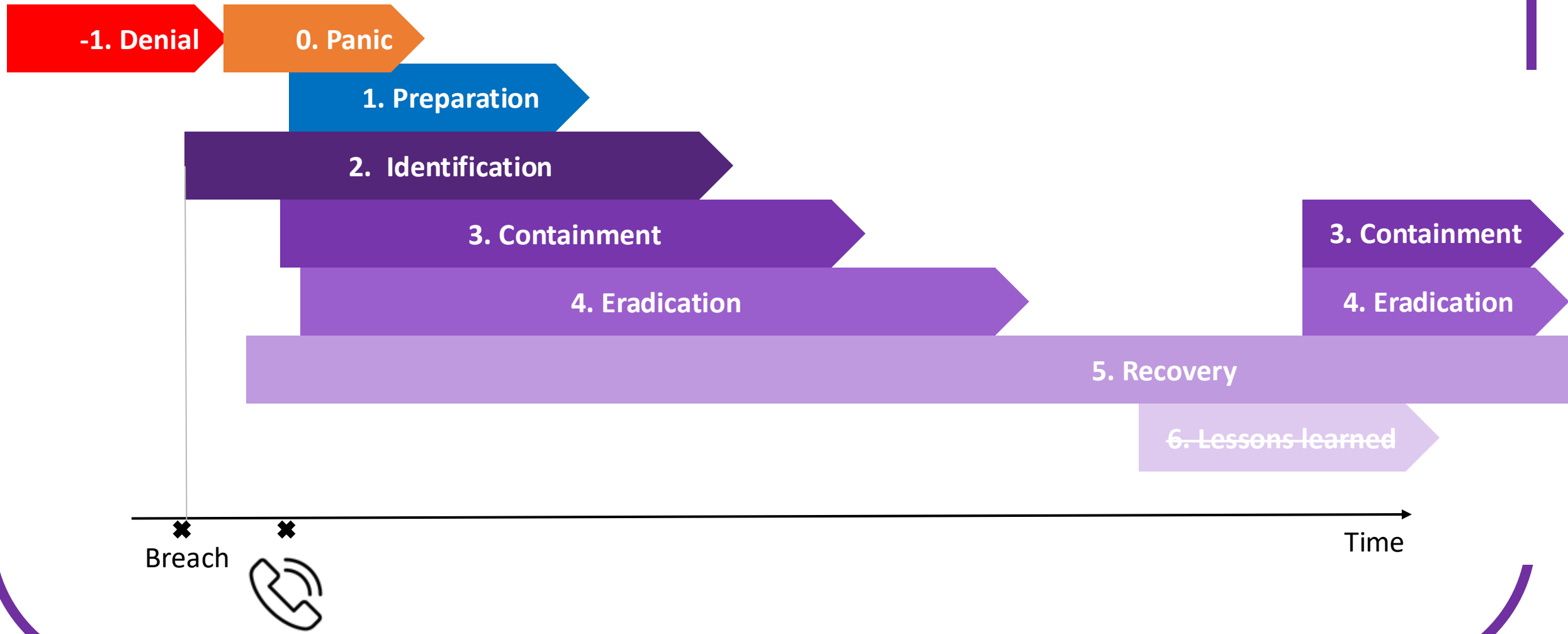
3 Capitalize

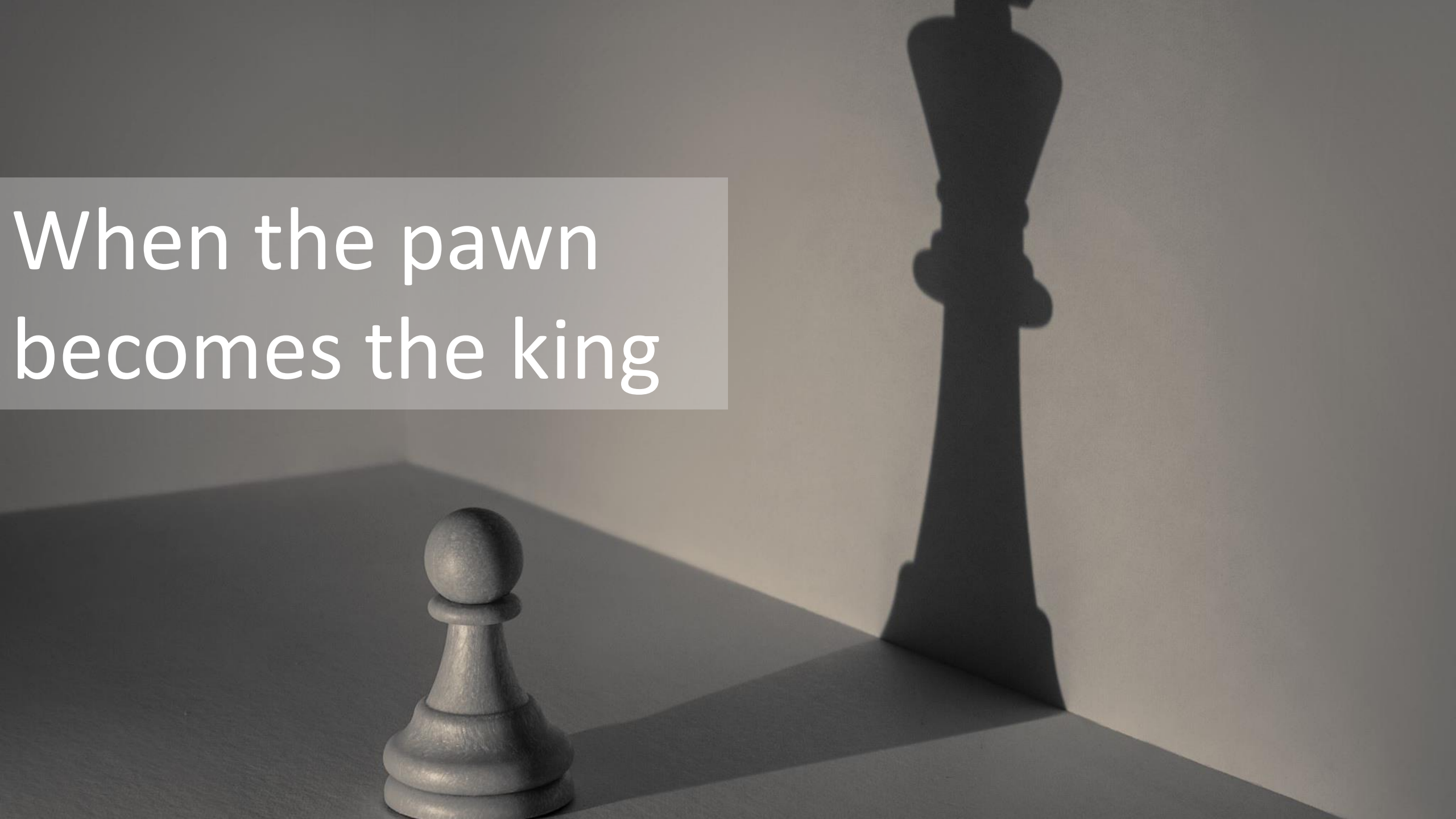
Exfiltrate valuable data
Inflict Damages

Responding to an incident

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

Reality is often quite different…




When the pawn
becomes the king

CASESTUDY – Sovereignty of technology

In a hyperconnected supply chain, **a sense of control is often assumed blindly**. But this is often an **illusion**.

Supply chains rely on digital infrastructure.

That infrastructure is often hosted, managed, and governed by third parties.

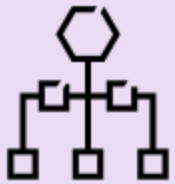
Misplaced trust in these providers can lead to catastrophic vulnerabilities.

Your 5 no-regret steps to building resilience

1

Establish resilience governance

Build governance structures to oversee and drive resilience.



2

Identify what matters most

Define the essential products and critical services that will form the baseline of your resilience programme.

3

Build resilience

Determine the resilience requirements of your critical products / services, and develop resilience capabilities accordingly.

4

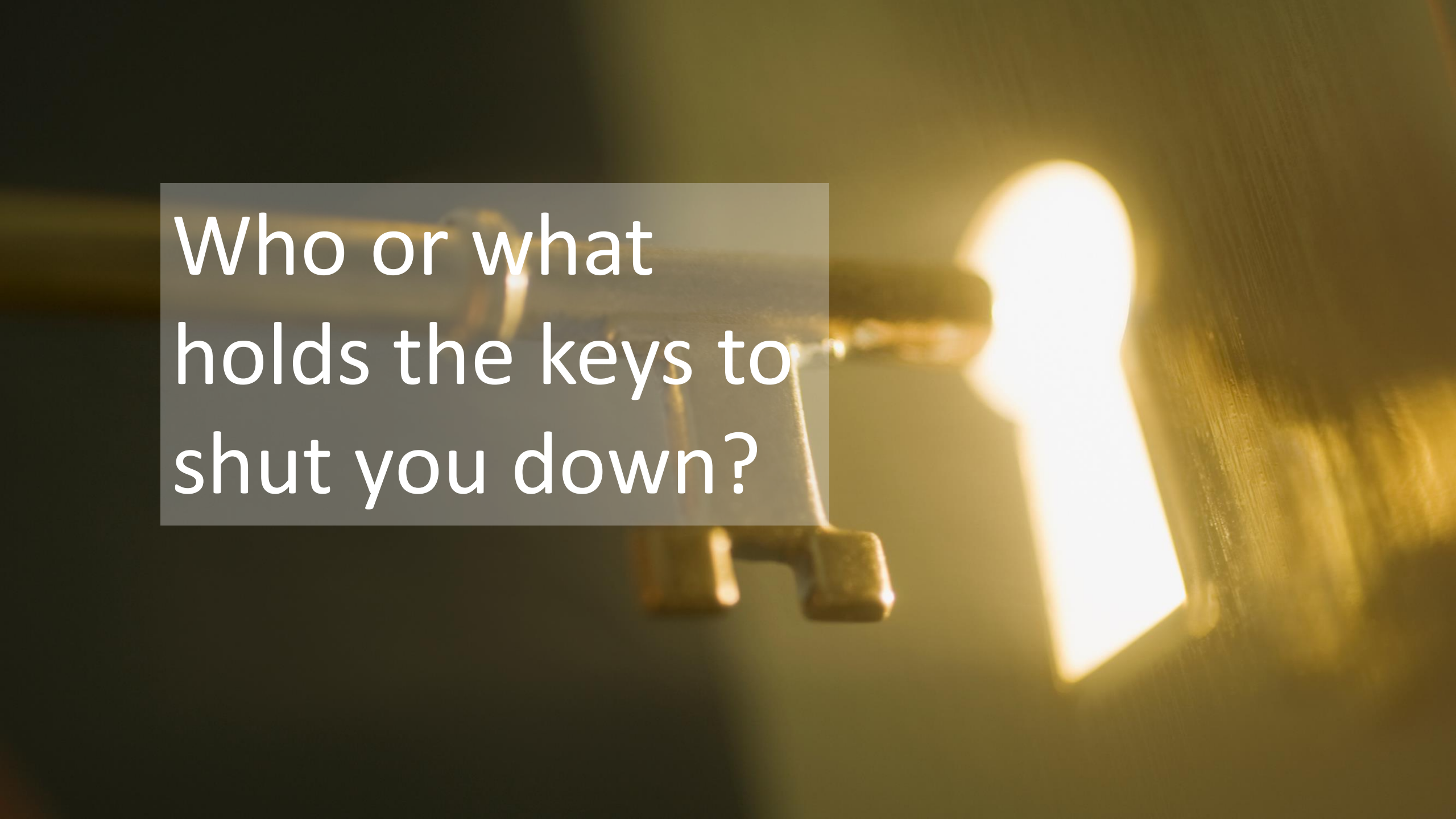
Build crisis management capability

Build a capability to manage unplanned or unprecedented scenarios. Develop a rapid incident reporting capability and crisis communications plan.

5

Embed and rehearse

Train your people and stress-test your resilience using scenarios aligned to your principal risks.


Who or what
holds the keys to
shut you down?

CASESTUDY – Sovereignty of technology

Digital sovereignty

Data sovereignty		Technological sovereignty
Where are data stored and computed?		Where is tech deployed and made resilient?
Who can access and use data?		Who designed, developed and operates the tech?
What laws and regulations apply to my data?		How does legislation affect the tech? (limitations, forbidden, sanctions)

Your cloud infrastructure

Reality

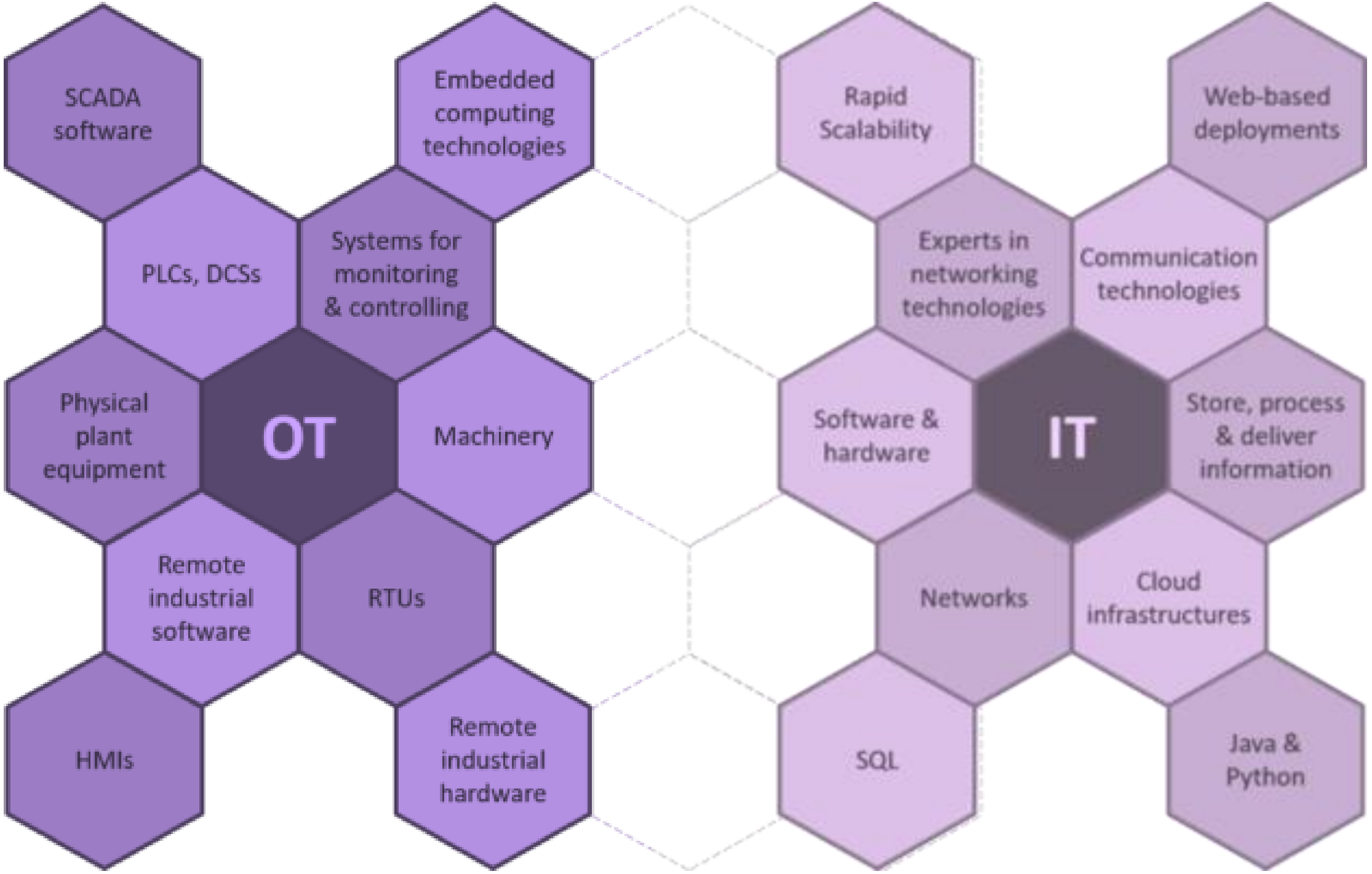
.EU organisations are shifting away from U.S.-based cloud providers due to concerns over foreign surveillance laws (e.g. CLOUD act) or geopolitical power shifts

Resilience impact

Data may be subject to external jurisdiction, risking confidentiality, compliance and operational continuity during geopolitical tensions. Your data is out of your hands. Trust is an important currency.

Actions

- Audit your cloud providers on compliance and include contractual resilience obligations
- Explore EU-based cloud alternatives for critical dependencies
- Implement data localisation policies.
- Include tech/data sovereignty in risk assessments and vendor selection.


SCADA software
Embedded computing technologies
PLCs, DCSs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
HMIs
Remote industrial hardware
Rapid Scalability
Web-based deployments
Experts in networking technologies
Communication technologies
Software & hardware
IT
Store, process & deliver information
Networks
Cloud infrastructures
SQL
Java & Python

Smart sourcing for increased control

Reality

Europe’s reliance on foreign technology (cars, batteries, solar panels and convertors) poses a major risk in terms of control and sovereignty of tech.

Resilience impact

A trade conflict or export restriction could paralyse entire sectors. Moreover, the producers or maintainers of this technology often have the power over these pieces of technology in the form of remote software control. We live in a house to which our landlord has the keys.

Actions

- Map your supply chain technology dependencies.
- Include sovereignty as part of your risk assessment and business case.
- Explore investments in alternative technologies and suppliers.

Who supplies the supply chain?

CASESTUDY – who supplies the supply chain?

Resilience requires **visibility**, **diversification**, and **preparedness**.

Influence is about **who shapes your operations**—often without your awareness.

The goal is to shift from **passive reliance** to **active influence** over your supply chain with **trust as currency.**

CASESTUDY – Supplier redundancy

Suppliers create value but also exposure. Influence is understanding who you rely on and how to leverage that in your favour.

Modern supply chains are built on **specialisation** and **outsourcing**.

There is deep dependency on **external** players, some of whom are **invisible** until they fail.

Who do you work with? And who do they work with? Is the supplier of your supplier (etc) aligned with your way of working? Is he even aware?


You outsource control,
but not responsibility
Do you have blind faith?
Or do you give faith a hand?

Automated warehousing dependency

Reality

Many companies **outsource** warehouse operations to third-party providers using **automated systems**: PLC's, automated storage, picking & retrieval, goods-to-person, automated conveyors/sortations, drones, cartesian gantry…

Resilience impact

A failure in the provider's systems, whether technical, financial, or operational, can halt distribution and fulfilment. These automated systems become a **"black box"** that cannot be touched by anyone but the supplier or certified experts.

Actions

- **Identify** critical warehousing **partners** and assess their **risk profile.**
- **Establish contingency plans** and manual fallback procedures.
- Make up-front **agreements** on recovery, roles, responsibilities…
- Consider **partial insourcing or dual-provider models**.
- Aim for **clarity**: do you know how long it would take to replace key PLC's?

(Rolling) stock ownership

Reality

Logistics firms increasingly rely on **external** providers for **transport assets** (trucks, railcars, etc.) and **components** to be used in the main production **lines** and **plants**.

Resilience impact

Cyber attacks, strikes, bankruptcy, or service disruptions of key suppliers can leave organisations without **delivery capacity**. If mismanaged, you are **'at the mercy of'.**

Actions

- Maintain a minimum **stock**, fleet or access to emergency transport.
- **Involve providers in business continuity planning.**
- **Monitor** financial health and labor relations of key **partners**.
- Include cyber resilience in **supplier audits**.

Power grid dependency

Reality

Most operations **assume uninterrupted access to electricity**, yet (the risk of) regional blackouts is increasing due to climate events and grid instability. Even in a unified Europe, countries will **first secure their own supply chain**, as we have seen during COVID. (IMERA)

Resilience impact

Data centers, manufacturing lines, and logistics hubs can be **paralyzed** without backup systems. This will affect **communication** lines, **continuity** and **restoration** capability.

Actions

- Invest in UPS systems and backup generators.
- **Prioritise critical sites** for infrastructure upgrades.
- **Exercise**! Include utility failure **scenarios** in crisis simulations.
- Have a contingency plan that allows for workarounds but assess if prolonged bypass doesn't create more errors than postponing resumption of activities.

EU resilience regulations

Critical Entities Resilience Directive (CERD) — In force

All hazards risk management **to reduce vulnerabilities and increase security** of entities whose services are deemed crucial to society.

NIS 2 Directive — In force

Developing and harmonizing cyber requirements for EU critical infrastructures.

Digital Operational Resilience Act (DORA) — In force

Harmonizing ICT risk requirements for the financial sector to mitigate cyberattacks and other risks.

Cyber Resilience Act (CRA) — In force

Addressing the security of hardware and software products with digital elements.

Internal Market Emergency and Resilience Act (IMERA): — On the horizon

Establishes a framework of harmonised measures to effectively anticipate, prepare for and respond to the impact of crises on the internal market. It focuses on critical dependencies, supply chain disruptions, and continuity of essential services, providing a coordinated EU response to crises that threaten market stability.

The Cyber Resilience Act

What does it aim to tackle?

1. The current low level of cybersecurity of **products with digital elements**, and
2. The insufficient understanding of consumers and access to information, standing in the way of choosing products with adequate cybersecurity properties.

What does it apply to?

EU and non-EU companies

1. manufacturing,
2. distributing,
3. importing

products with digital elements in the European market

Products with digital elements:

“ whose intended or reasonably foreseeable use involves direct or indirect logical or physical data connection to a device or network”

What does it address?

Security by design

- Resilience testing
- Technical testing
- Software review
- Documentation of compliance and certification
- Firmware assessment
- Continuous security updates

Risk management

- Mandatory regular risk assessments and remediation of any identified vulnerabilities within 24 of being found.

Information disclosure

- Users: clear informed about security updates and known vulnerabilities.
- Supervisor: detailed reporting of discovered vulnerabilities/incidents.

Today went well, what about tomorrow?

Musk shutdown Starlink service during Ukraine counteroffensive - report

Reuters report claims the blackout hurt Ukraine's efforts in Kherson

July 30, 2025 By: Paul Lipscombe Have your say

Elon Musk reportedly ordered Starlink to cut Internet coverage in parts of Ukraine during a counteroffensive in the earlier stages of the Russian invasion.

A Reuters report earlier this week, which cited three sources, said Musk ordered a senior SpaceX engineer to cut coverage in areas including Kherson, a strategic region north of the Black Sea that Ukraine was pushing to reclaim back in 2022.

09 Jan 2024

Rebuilding Ukraine’s telecoms infrastructure amid war

The decision disrupted Ukraine's counteroffensive efforts and has strained the country's trust in Starlink.

“We have to do this,” Michael Nicolls, the Starlink engineer, told colleagues upon receiving the order, one of the sources told Reuters. Details around how long the outage lasted were not clear.

It's claimed that at least a hundred Starlink terminals were deactivated, while the decision also impacted other areas seized by Russia, including some of Donetsk province further east.

Wake-up call: Microsoft sluit e-mail ICC zonder pardon af

Als de Tweede Kamer iets besluit wat Washington niet zint, kan de toegang tot parlementaire e-mail op bevel worden afgesloten.

Sjoerd Hartholt 19 mei 2025

Microsoft. – Shutterstock

Zonder tussenkomst van een rechter, zonder bezwaarprocedure en zonder dat het ICC zich kon verweren blokkeerde Microsoft op last van de Amerikaanse overheid vorige week de toegang tot onder meer e-mail van hoofdaanklager Karim Khan van het Internationaal Strafhof (ICC). Het voorval leidt in Europa tot grote zorgen over de Europese digitale afhankelijkheid. Dat meldt persbureau Associated Press.

De aanleiding voor de sancties zijn de arrestatiebevelen die het ICC uitvaardigde tegen de Israëlische premier Netanyahu en oud-minister Gallant, in verband met mogelijke oorlogsmisdaden in Gaza. De regering-Trump beschuldigde het hof van politieke motieven en beperkte via sancties de bewegingsvrijheid van ICC-

FTC, States Sue Deere & Company to Protect Farmers from Unfair Corporate Tactics, High Repair Costs

Deere's monopoly practices unfairly drive up farming equipment repair costs, restrict farmers ability to quickly seek repairs necessary for planting, harvesting

January 15, 2025

Tags: Competition | Bureau of Competition | Nonmerger | Single Firm Conduct | Unfair Methods of Competition | bundling | exclusionary conduct | Manufacturing | Industrial Goods | Food and Beverages | Exclusionary Conduct

The Federal Trade Commission today, along with the Illinois and Minnesota Attorneys General, sued agricultural equipment manufacturer Deere & Company (Deere) over its use of unfair practices that have driven up equipment repair costs for farmers while also depriving farmers of the ability to make timely repairs on critical farming equipment, including tractors.

The FTC's complaint alleges that, for decades, Deere's unlawful practices have limited the ability of farmers and independent repair providers to repair Deere equipment, forcing farmers to instead rely on Deere's network of authorized dealers for necessary repairs. This unfair steering practice has boosted Deere's multi-billion-dollar profits on agricultural equipment and parts, growing its repair parts business while burdening farmers with higher repair costs, the FTC's complaint alleges.

"Illegal repair restrictions can be devastating for farmers, who rely on affordable and timely repairs to harvest their crops and earn their income," said FTC Chair Lina M. Khan. "The FTC's action today seeks to ensure that farmers across America are free to repair their own equipment or use repair

Related Cases

Deere & Company, FTC v.

Related actions

Statement of Chair Lina M. K
the Matter of Deere & Compa

Dissenting Statement of
Commissioner Andrew N. Fe
Joined by Commissioner Me
Holyoak In the Matter of Dee
Company

Topics

Food Marketing to Children a
Adolescents

Single cloud provider risk

Reality

Organizations often rely on one cloud vendor for hosting, storage, and compute services.

Resilience impact

A service outage, legal dispute, or breach can cascade across all digital operations. Especially single-source dependencies are vulnerable to cascading operational disruption.

Actions

- Use multi-cloud or hybrid cloud strategies.
- Segment workloads by criticality and provider.
- Regularly test failover and recovery capabilities.

I see, I see, what you don’t see…

CASESTUDY – Translating big picture stuff into concrete risks and impacts

Reality

Organisations may lack awareness and vision on trends and developments that affect both your strategy and risk landscape on the mid to long term.

Resilience impact

- Regulatory non-compliance
- Ill preparedness to proactively identify, mitigate and prepare for impacts
- Delayed response to (geopolitical) cyber threats (e.g. sanctions, data localization laws) can disrupt operations or trigger penalties.

Actions

- Establish a process to continuously identify long term risks and trends.
- Monitor regulatory changes across jurisdictions.
- Align cybersecurity policies with emerging legal frameworks.

CASESTUDY – Translating big picture stuff into concrete risks and impacts

Reality

Some utilities and energy firms use horizon scanning to anticipate environmental disruptions (e.g. floods, heatwaves) that could expose vulnerabilities in operational technology (OT) systems

Resilience impact

Environmental stressors can trigger cascading failures in OT networks, especially if cybersecurity controls are not adapted to physical risks.

Actions

- Expand your risk sensing and identification capability into OT cybersecurity planning.
- Segment OT networks and ensure encrypted local control.

Turning strategic resilience into operational resilience

Tool	Purpose	Practical Tip
Horizon scanning	Identify emerging risks early	Use external intelligence platforms and internal expert networks. Combine strategic foresight with operational metrics
Automated trend tracking	Monitor real-time signals obtain early warning indicators	Integrate dashboards with supply chain KPIs and external feeds
Scenario modelling	Simulate disruptions and responses	Run tabletop exercises and stress tests quarterly

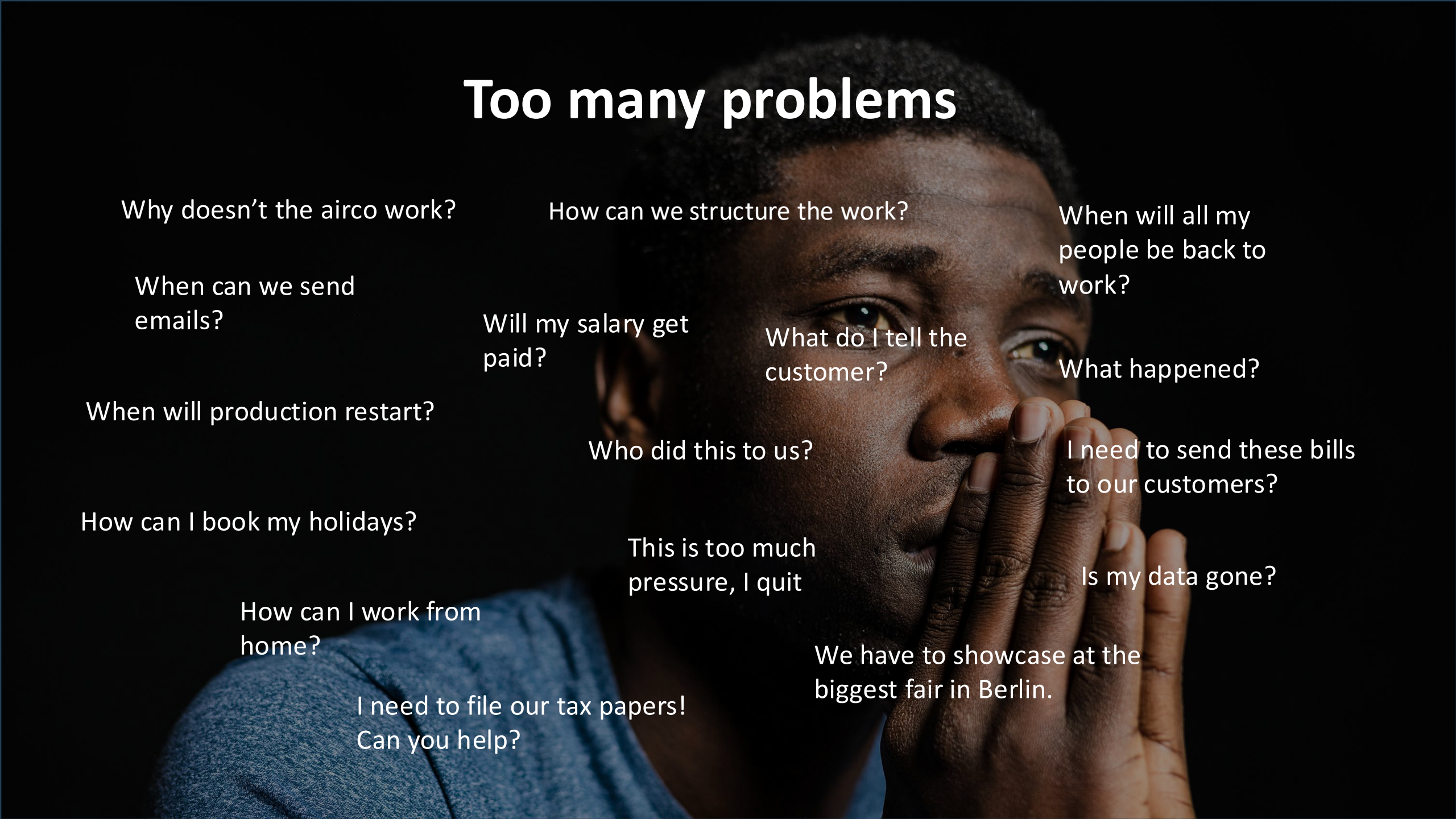
Cross-functional ownership!

Document assumptions

Regulatory changes.


It’s about
the people

Too many problems



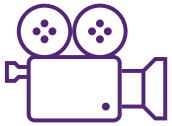
It’s about the people!

Psychological impact of going through a cyber attack

Relief management

Workforce fatigue

Brain drain: keep your skilled people on board!



Media scrutiny

Legal breaches (e.g. GDPR)

Extortion of next of kin

Key takeaways

What you should remember after today:

Business leaders recognise that a foundation of resilience can make the difference between faltering or flourishing. Consider:

1

What is your **minimum viable company**/supply chain? Ensure you have a plan B in place. **Test** this.

2

Revisit your risk profile and appetite.

Consciously readdress your risks in an integrated manner.

3

Am I able to seize an opportunity when it presents itself on the horizon? Am I "agile enough"?

Let’s build a more resilient world

Thank you for your attention!

Next SLF event

SERVICE LOGISTICS FORUM

27 november 2025

Service Leadership Summit

Service Logistiek in tijden van Schaarste

Register:

THANK YOU!