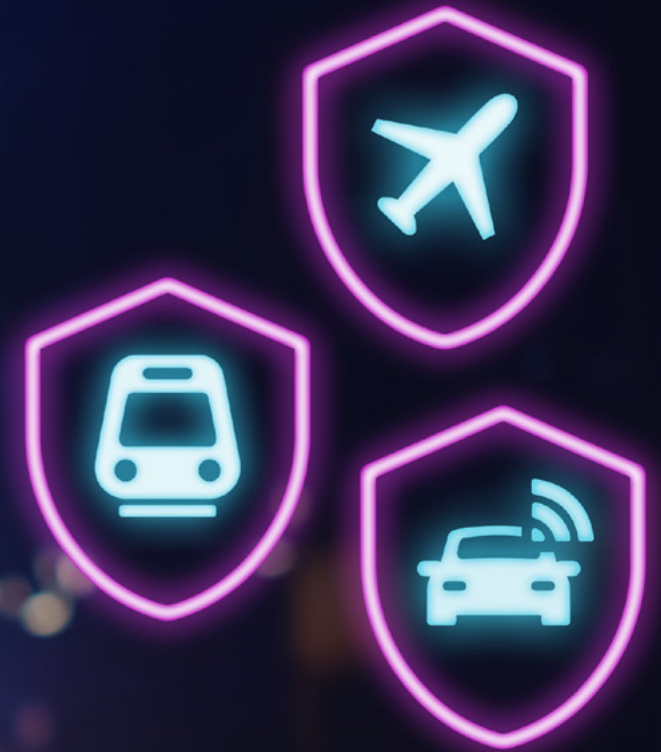


# Cybersecurity for safe mobility

The essential guide  
for industry  
executives and  
engineers



# Cybersecurity 101, an introductory course for all people working in Transportation and Mobility.

Cybersecurity has reached a tipping point. For a long period of time, cybersecurity issues were mainly associated with IT, but as the impacts on passengers' safety are now rising, cybersecurity is on the agenda of most executive leadership teams within the transportation industry. As transportation systems are increasingly connected to the rest of the world, they are more vulnerable to cyber-threats. A whole suite of new cybersecurity regulations and enforcement is on the horizon for the transport industry, accelerating the deployment of cyber strategies for the sector.

Thanks to years of practicing and learning in this industry, Expleo identified the keys areas to successfully implementing effective cyber defences 1 – consciousness of existing and potential threats, 2 – executive leadership to address these cybersecurity threats, and 3 – tight cross-organisation collaboration in delivering end-to-end cyber resilience over the value-chain.

**“It is time to move to a new paradigm where from the outset, cybersecurity issues are taken into account, breaking the barriers between engineering and manufacturing, onboard system developments and offboard digital services, as well as strategic and operational roles.”**

We observed, designed and implemented best practices to create Expleo's first cybersecurity guide dedicated to all people working in the automotive, railway, and aerospace industries. It provides an overview of cyber-threats and forthcoming regulations and the ways in which to adapt. The guide provides simple managerial and technical concepts, good cybersecurity practices applicable to all transport industries, as well as digestible infographics for the non-technical reader. It is the first guidebook of a cybersecurity series: the following ones will dig into case studies that address issues specific to the railway, aerospace, and automotive industries.

We hope our guide will enable your organisation to focus on the pressing cybersecurity projects in your industry.



**HERVÉ GARNOUSSET**

Global Head of Digital Solutions  
at Expleo Group

# Content

- Vehicle cybersecurity by the numbers** ..... 4
  
- STEP 1 – Cyber Threat in the mobility sector: know your enemy and yourself** ..... 6
  - 1A Cyber attacks in the mobility sector – who leads them, how and why?..... 7
  - 1B Exploring the attack surfaces of connected mobility solutions ..... 10
  - 1C Understanding six types of cyber-threats with the STRIDE model ..... 11
  
- STEP 2 – Cybersecurity compliance in the Mobility sector: what you need to know** ..... 12
  - 2A Cyber regulations for the mobility industry: your 2023 to-do list..... 13
  - 2B Cybersecurity compliance: the eight key stakeholders ..... 14
  
- STEP 3 – Cybersecurity action plan: how to build it in the mobility industry** ..... 16
  - 3A The critical success factors for the mobility industry’s leaders..... 17
  - 3B The security action plan and best practices for the mobility industry’s engineers ..... 20
  
- Takeaways** ..... 23



# Vehicle cybersecurity by the numbers

BE CONNECTED EVERYWHERE BUT...

**225%**

increase in the frequency of cyberattacks on cars from 2018 to 2021.

Upstream Automotive  
Cybersecurity Report 2022

**85%**

of the attacks on cars are carried out remotely.

Upstream Automotive  
Cybersecurity Report 2022

**5.3  
billion  
per year**

the number of European train passengers accessing onboard Wi-Fi by 2028.

It will grow to nearly five times its current usage levels.

BWCS Research 2019

## ARE YOU SECURED BY DESIGN?

**40%**

respondents of the aerospace industry haven't incorporated cybersecurity into the earliest stages of their projects.

AIAA Cybersecurity survey 2020

**\$1  
million**  
**1  
year**

the cost and length of time it takes to change and implement one line of code on a piece of in-service commercial aircraft's avionics equipment.

U.S. Department of Homeland Security – Cyber Security Division

**100  
million**

the number of lines of code in a recent premium car, executed on 70-100 electronic control units (ECU) networked.

Manfred Broy, Professor of software engineering, Technical University Munich

## SMALL BREACHES LEAD TO BIG CONSEQUENCES

**15,000**

travellers were affected as the ticketing system of the Danish rail operator (DSB) was paralysed by a DDoS attack in 2018

**9  
million**

EasyJet passengers had their data illegally accessed in 2020 as part of a sophisticated cyberattack and had to pay customers significant compensation.



**Cyber threat in the mobility sector**

**Know your enemy and yourself**

## 1A | Cyber attacks – who leads them, how and why?

**“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”**

Sun Tzu, The Art of War

In other terms and within the realm of cybersecurity and vehicle systems, knowing your attackers better can help identify which of your resources are valuable to them, why they would target them, and how they would proceed. The objective: enable your organisation to better protect its assets from them.

## Researchers and hobbyists

These actors can be academics, ethical hackers, or other individuals that are interested in researching cybersecurity vulnerabilities not solely to expose them, but rather to demonstrate how the investigated system’s defences can be improved. They typically are the first hackers to attack a new system or device, and work with the sole purpose of learning and teaching good cybersecurity practices. Their research results are usually shared as a B2B service, online, or during conferences, a practice also called ‘open security’ that has proven to be useful for testing any vehicle system’s cybersecurity level of robustness.



## Pranksters and hacktivists

These people have the same skills as described above for researchers and hobbyists, but with different motivations as they are looking for media coverage, or some level of visibility, by exposing an organisation’s vulnerabilities. They usually lack the resources to effectively attack a vehicle system due to its complexity, but if they are financed by criminal organised groups, they can go as far as attacking railway systems as such tactics are large-scale and highly visible.





## Owners and operators

This category reunites various profiles of individuals that hack a vehicle they own. It could be a car owner that wishes to improve his vehicle's speed performance by removing restrictions imposed by the manufacturer or government regulator, or someone that simply wishes to repair his car by itself. They can also have more dubious motives for hacking a system by disabling some of its components, like hiding their identity if they stole the vehicle.



## Insiders

An insider is someone with access to the organisation's or the transport system's critical information. It can be an organisation member, or a hacker accessing the account of a team member, thanks to spoofing or elevation of privilege techniques. He can be asking for money and threaten to leak the sensitive information he found in the media, an industry competitor, etc.



## Organised crimes

These attackers are motivated by financial gains and their most common way of attacking a system is ransomware, which can lead to double or triple extortion (they take possession of a system first, of its employees' data second, and its users last). An example of an organised crime attack could be paralysing a vehicle's system with DoS and asking its owner for a ransom before allowing its reboot. They can even employ the Ransomware-as-a-Service (RaaS) model where they sell their hacking skills to other criminals.



## Terrorists and activists

Activists can work individually or as organised groups, to provoke political and social change (e.g. human rights, freedom of speech, environmental issues) by acting against the principles of certain organisations and governments. Their most common technique is leaking sensitive data or blackmailing the victim of the attack in private until the target changes its behaviour, secretly extorting sensitive information, employing Distributed Denial of Service (DDoS) to freeze a system like an airport, or hacking X-ray or CCTV systems to allow people or prohibited objects to go through security gates unseen.



## Nation-states

A government's most common motives are industrial espionage, surveillance, and economic or physical warfare. Their goal can be to steal intellectual property, disrupt the delivery of a new product, compromise product performances, etc. Nation-states could be interested in hacking another government member's car to spy on it, attacking embedded systems for political or military purposes, or damaging critical transportation infrastructures.



## What are honeypots?

A honeypot is a cybersecurity mechanism used by organisations, including Expleo, that consists of simulating targets, such as connected Industrial Control Systems, to lure cybercriminals away from real targets and observe their tactics. The benefit of a honeypot is not only the protection of an existing system, but also improved anticipation of possible future attacks on similar systems.

# 1B | Exploring the attack surfaces of connected mobility solutions



- 1 OT systems (ICS, SCADA & PLC)**
  - Road traffic control centre
  - Rail operating centre
  - Air traffic control centre
- 2 Infrastructure & IoTs**
  - Connected Vehicle Traffic Signal System (e.g. V2I)
  - Interlocking systems & balises
  - Airport Landing Aids, Guidance and Lighting
- 3 Cloud & IT infrastructure**
  - Ground connection based on mobile network technology (e.g., GSM-R & Radio Block centre), Operator's IT and Manufacturer's data platform (e.g. Airbus Skywise)
- 4 Satellite**
  - Global Navigation Satellites Systems (GNSS) and Satellite Communication (SATCOM)
- 5 Aircraft**
  - Automatic Dependent Surveillance-Broadcast (ADS-B) system, on-board WiFi connections and infotainment systems
- 6 Train**
  - On-board ATP (Automatic Train Protection), Train control management system (TCMS), & on-board Wi-Fi entertainment system
- 7 Car**
  - Keyless entry system, on-board diagnostic system (CAN), eCall (4G) system, TPMS, ADAS sensors (Radar, Camera, Lidar) and on-board infotainment system
- 8 Employees & Passengers**
  - Web and Mobile App (ticketing, passenger information system...)

# 1C | Understanding six types of cyber-threats with the STRIDE model

STRIDE is a framework developed by Microsoft to help engineers identify their products' vulnerabilities according to six threat categories which are not mutually exclusive.




	<b>S</b> <b>SPOOFING</b>	<b>T</b> <b>TAMPERING</b>	<b>R</b> <b>REPUDIATION</b>	<b>I</b> <b>INFORMATION DISCLOSURE</b>	<b>D</b> <b>DENIAL OF SERVICE</b>	<b>E</b> <b>ELEVATION OF PRIVILEGE</b>
	Consists of the attacker impersonating a legitimate entity to deceive a target. For example, an attacker can impersonate a legitimate satellite navigation system by transmitting a GPS signal to a drone. The drone's location and autonomous navigation will be disrupted if this signal contains incorrect coordinates.	Involves altering data in a system to cause different behaviour. For example, an attacker who manages to modify the value of a train's instantaneous speed in the system could make the driver believe that the train is travelling at an authorised speed when in reality, it is well above that limit.	Is erasing all traces of one's malicious actions within a system. For example, an attacker who has managed to break into the operating system of a drone will target the log files within the system to remove all references to his connections and commands. Conversely, non-repudiation prevents the history of actions performed within a system from being modified, for example, by associating a user's actions with their digital signature.	Is the malicious exploitation of insufficiently protected data within a system. For example, an airline website that has not configured sufficiently restrictive rights to access its files or whose database queries are displayed to the user in error could allow an attacker to steal the data of the airline's users, including credit card information.	Is an attack that consists of saturating a system with requests using malicious programs to monopolise it and thus prevent it from delivering its service to legitimate users. For example, a denial of service attack on a train company's reservation site could prevent the sale of tickets, therefore disrupting traffic.	Consists of an attacker exploiting a system's vulnerabilities to increase the rights of an account they have, allowing them to access critical operations and data. For example, exploiting a vulnerability of a connected car's media management system made it possible to temporarily obtain administrator rights from a standard user account and thus control the vehicle.
<b>Property violated</b>	Authentication	Integrity	Non-repudiation	Confidentiality	Availability	Authorisation
<b>Ex</b>	Hijacking, Replay, Brute Force	Cross-Site-Scripting, SQL Injection, Firmware modification	Repudiation Attack, Stealth Attack	Trojan Horse, Spyware, Reverse Engineering, Cryptanalysis, Port Scanning, Side-channel-Attack	DoS, DDoS, Jamming	Buffer Overflow, Rootkit, Backdoor



**Cybersecurity compliance  
in the mobility sector**

**What you need to know**

## 2A | Cyber regulations for the mobility industry: your 2023 to-do list

National & supranational legislations <b>NIS1/NIS2 &amp; National Regulation</b>		✓
Personal data protection regulations <b>GDPR (EU) &amp; Privacy Shield (US)</b>		✓
Payment security standards <b>PCI DSS</b>		✓
IT cybersecurity standards <b>ISO 27K Family &amp; NIST SP800</b>		✓
Cryptography & IoT security standards <b>FIPS 140, ETSI EN 303 645 &amp; Common Criteria 15408</b>		✓
OT (industrial automation & control systems) security standards <b>IEC 62443</b>		✓
Railway applications – cybersecurity <b>CENELEC prTS 50701</b>	Automotive security standards for ISO <b>ISO/SAE 21434, ISO 24089</b> UNECE Vehicle Regulations <b>UN R155, UN R156</b> <b>GB/T OIIS 204-10</b>	Airworthiness security standards <b>EUROCAE – ED201, ED202A, ED203, ED204</b> Information security for organisations supporting civil aviation operations <b>CEN prEN 16495</b>
 ✓	 ✓	 ✓

Following cybersecurity compliance standards can seem complex, but professional support is available to help.

That expertise is invaluable: complying with regulation is not only required to put products on the market, it exists to ensure the safety of all.



## 2B | Cybersecurity compliance: the eight key stakeholders

New compliance rules relating to cybersecurity in the transport industry push all the sector's stakeholders to ensure their products are compliant. Even though cybersecurity compliance standards can seem complex, such expertise is invaluable: respecting regulations is not only necessary to put products on the market, they most importantly exist to ensure the safety of all.

As cybersecurity regulations affect all actors of the product chains – from design to production to distribution – we're keeping it simple with a list of eight key stakeholders that you can find in the railway, aerospace, and automotive industries.

## Integrated systems and equipment suppliers

Designate all actors that intervene within the supply chain of the entire vehicle ecosystem: embedded, IT and Industrial Control Systems. It includes Original Equipment Manufacturers (OEMs) – meaning system, component, software and hardware suppliers – and any relationship between IT and hardware vendors, hardware component makers, software vendors and channel partners such as resellers and distributors.



## Transport operators

Such as airlines, rail operators, logistical and road companies, or any organisation that operates an activity that requires exploiting the transport data and service.



## Infrastructure operators or traffic management systems

E.g., train stations, airports, and any entity in charge of traffic control or signalling of the transport network.



## Service providers

Comprise all third parties contracted by the infrastructure and transport operators, e.g., Expleo and its engineering consulting services or IT integration and monitoring offers, maintenance services such as MRO, and fleet management services.



## Authorities and bodies

Any organisation in charge of enforcing cybersecurity policies and regulations, compliance approval. For example, railway regulators, national and European authorities for safety and cybersecurity, and conformity assessment bodies.



## Public areas

That use transport premises to offer services to passengers and manage passengers' data and information.



## Distribution channels

Such as car dealerships, freight, car rental services, travel agencies, tourist brokers, etc.



## Other entities

Organisations that have a contractual relationship with the transport infrastructure stakeholders, which involves sensitive information, like railway freight insurance companies or banks.





**Cybersecurity action plan**

**How to build it in the mobility industry**



## 3A | The critical success factors for the mobility industry's leaders



What is the key to a successfully secured vehicle ecosystem? Its management's capacity to spread and centralise good cyber practices amongst all teams and **make the product engineering and IT departments work together**. Why? It's the only way to make sure that all your components, embedded systems and their interdependencies are secured.

**The Zero Trust (ZT) approach is not only the most welcomed way to protect valuable assets, it is essential as it can easily be adapted to any organisation's specifics.**

### What is the ZT approach?

Zero Trust is a set of cybersecurity principles that move cyber defences from static, network-based perimeters, to focus instead on users, assets, and resources.

Hence, a Zero Trust Architecture (ZTA) considers all users as potential threats and prevents access to data and resources until they can be properly authenticated, and their access authorised.

In short, a ZTA covers industrial components, local networks, cloud networks, web applications, devices, hardware components, embedded software, communications, mobile and web applications, and employees/users in any location.

## How to implement the Zero Trust methodology?

Through the ZT approach, the management team must ensure that there is a commitment from all teams involved to follow a shared set of principles (listed below). To do so, it's vital to

1 – establish effective communication between IT and engineering teams so that they can

2 – discuss and implement cybersecurity defences throughout as well as

3 – evangelise all other contributors to the transportation system about such practices.

- **Assess risks thanks to the Threat Landscape approach.** The objective is to define the new perimeter and scope potential and existing threats affecting the transportation system. To do so, three elements are checked: 1 – the value of sensitive information available, 2 – the level of information security which is in place, and 3 – geopolitical factors (if it's pertinent to the product).
- **Put in place governance of authentication** by being as cautious as possible regarding workers turnover and the mobility of both workers and users. The goal is to **reinforce authentication processes.**
- **Organise all resources per segment** as the embedded devices, the embedded software, the SCADA systems, the communication systems, the IT infrastructure, etc. Moreover, it's essential to pay attention to the legacy systems: many of them, such as rail signalling systems, can be over fifty years old. In the past, there was a lack of concern about security and authentication in the design, deployment and operation of these systems.
- **Continuously update transportation systems' cyber defences** to adapt to their Threat Landscape as the latter is also constantly evolving.
- **Set up regular cybersecurity learning courses** for all people involved in the conception and the creation of the transportation system, preferably by creating learning groups composed of engineering and IT experts.
- **Build a trained team dedicated to security.** It should know how to log, archive and react to alerts in real-time, thanks to event management systems which monitor the totality of the transportation system's perimeter, round the clock.
- **Isolate each application within the embedded systems** with a separation kernel that breaks them into partitions. That way, partitions can't access each other's resources or data and if an attack targets one partition, the kernel will prevent it from spreading to other parts of the application.

**Such an effort is progressive and continuous, therefore centralised and effective security governance is vital to maintaining a robust transportation system architecture.**

**The best way to be  
100% secure?  
Cyber resilience testing.**

Thanks to thorough testing, engineering teams can summarise observed strengths and weaknesses. Regarding existing products, tests can only be retroactive. Still, it is ideal for integrating tech security testing into the Agile process while developing new ones, because it's always better to be safe than sorry!

Smeeta, the briefcase that will break into your system... if you let us

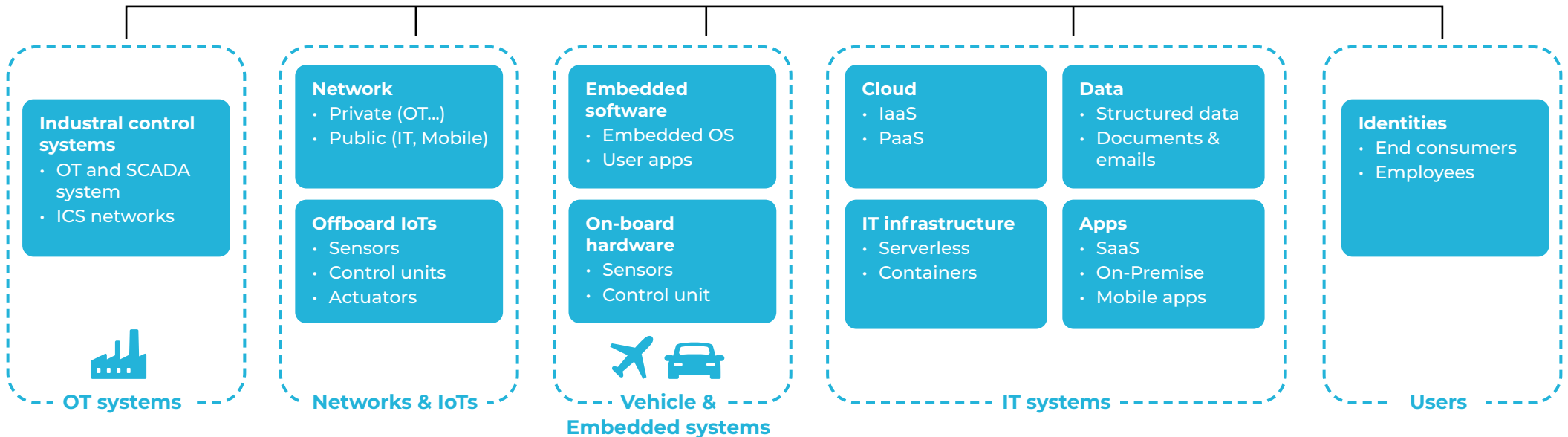
For R&D purposes, Expleo's cybersecurity experts designed Smeeta, a briefcase to test any transportation security system.

Smeeta can launch a cyber attack against a car or a drone, lead a security assessment to identify vulnerabilities and conduct forensics to compile evidence of an attack.



# 3 B | The security action plan and best practices for the mobility industry's engineers

<b>Risk Management</b> <ul style="list-style-type: none"> <li>• Continuous risk assessment</li> <li>• Continuous risk treatment and mitigation</li> </ul>	<b>Security policy</b> <ul style="list-style-type: none"> <li>• Governance management</li> <li>• Compliance management</li> <li>• Security assessment</li> <li>• Security controls &amp; hardening</li> </ul>	<b>Threat protection</b> <ul style="list-style-type: none"> <li>• Threat intelligence</li> <li>• Cyber resilience testing</li> <li>• Cyber forensics</li> </ul>
---	---	---



- Network segregation
- Hardening

- Secure the seven levels of OSI model
- Traffic filtering & segmentation

- Deploy secure SDLC
- Separation kernel
- Supply chain integrity
- Encryption IC
- Secure Boot/Authentication

- Hardening
- Classify, label & encrypt
- Runtime control (RASP)
- Adaptive access control

- Strong authentication
- Training & awareness

## Some best practices for implementing cybersecurity controls into your vehicle's ecosystem

Every effective cybersecurity strategy relies on three main pillars: a centralised management of security policy that gives direction to all teams to build robust cyber defences across the entire ecosystem, a 'vigilante squad' dedicated to threat protection that continuously updates the defences according to its research, and high-level risk management that analyses and mitigates threats. Once these three foundations are built, specific security controls can be taken to protect every component.



- The seven levels of the **Open Systems Interconnection (OSI)** model encapsulate all the layers used by computer systems to communicate over a network. It is essential to consider them to facilitate segregating IT networks and IoT. Although the principle of segregation also applies to OT systems.
- **Network segregation and filtering** consist of breaking the networks into layers and endorsing communication rules between them to mitigate cyber-attacks. Adding this complexity makes it more challenging for hackers to reach the most critical data. For example, isolating the system in charge of notifying train passengers about railway traffic from the one that handles actual traffic, is a cybersecurity must.
- A way of preventing data loss is to **classify, label, encrypt and control the access** of all the data if necessary. This approach involves listing all data per levels of sensitivity and enabling access to each category according to different security levels (e.g., more or less complex authentication, or users allowed to access the data, see adaptive access control below).
- **Adaptive access control** or privilege access control gives access to X layers and Y features to Z users, according to their identity. This practice is quite common for Cloud-hosted apps.

- To protect the identities of the organisation's employees and its products' end-users, it is necessary to enforce identity access management, Multi-factor Authentication (MFA) or other **authentication reinforcement** methods and teach best practices thanks to **cybersecurity training and awareness**.
- **Hardening** is a technique based on the logic of limiting risks thanks to optimisation – all unnecessary features are deleted, leaving fewer opportunities for attackers to be able to intrude and exploit the system. Hardening can be applied on low levels (as in a kernel or a TCP/IP stack) and global levels on operating systems, applications, or services, etc.

- **Secure Software Development Life Cycle (SDLC)** is a comprehensive methodology that considers cyber matters throughout the entire development of a vehicle or embedded system. It consists of but not limited to the following best practices: detecting anomalies specific to cybersecurity within the code, hardening and adapting the embedded system to its environment thanks to cyber threat-proof integration techniques, and integrating testing to all development phases.
- **Separation Kernels are Low-Level protection** including multiple Independent Levels of Security: Environment Sandboxing, Data/kernel Isolation, Damage Limitation, Periods Processing, Tamper Proof, Memory Protection, etc.
- Handling data flows with **Integrated Circuit encryptions (IC)** enables the embedded software to encrypt outgoing and decrypt incoming data.
- **Secure Boot, Secure Authentication, Secure Update, Secure Logging etc.**, are hardware and embedded systems-based security controls and mechanisms that ensure the highest level of protection is integrated into a system's environment.
- **Runtime control (RASP)** is a high-end monitoring system that automatically detects vulnerabilities where the system has been compromised to block threats even before they occur.
- Ensuring **supply chain integrity** means verifying all the components used, meaning all the suppliers the organisation partners with, and respecting compliance rules, from the microchip to the USB key, to the processor.

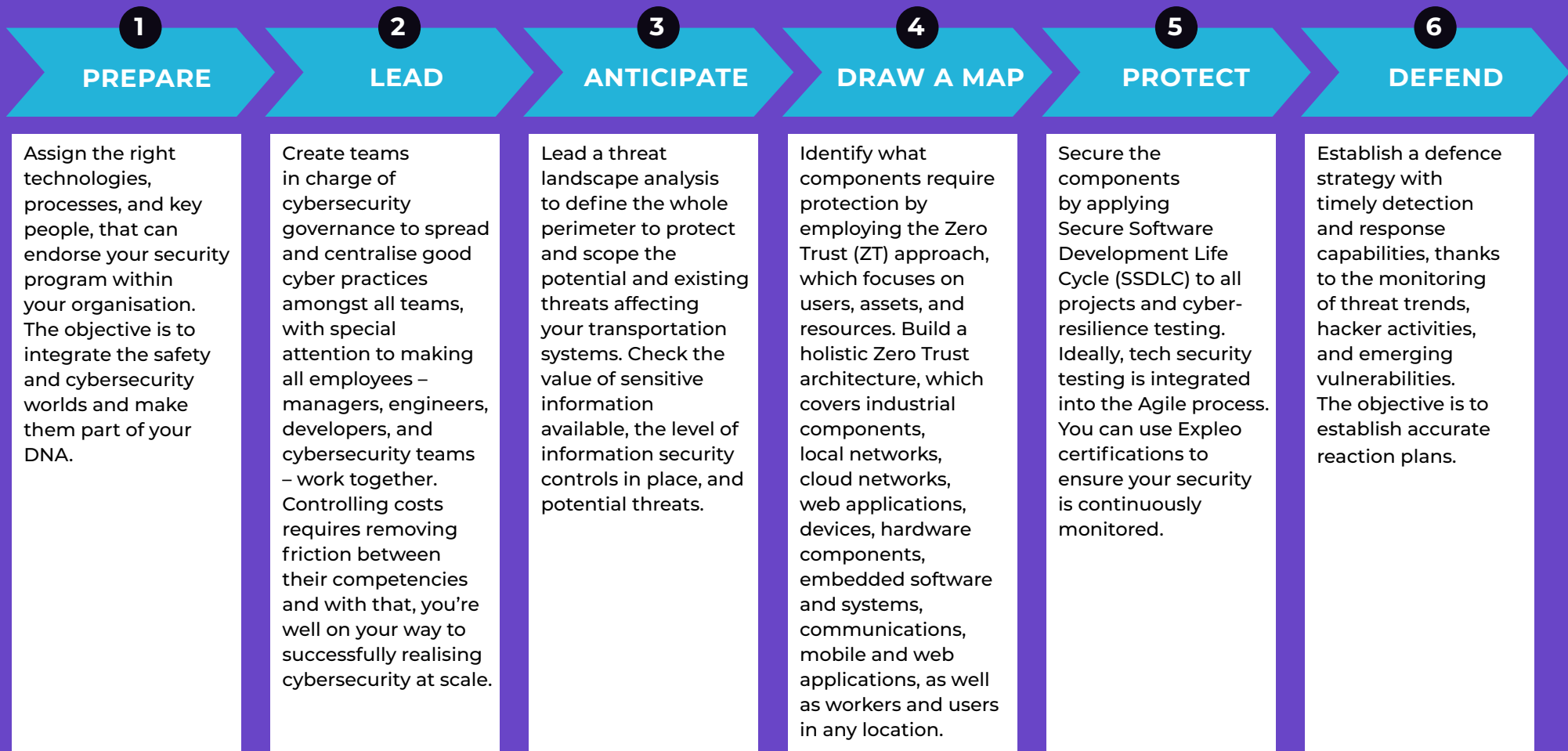


# Takeaways

Now that we have unpacked the main principles and good practices in cybersecurity, here are the steps we recommend you follow to implement them:



**HELMI RAIS**  
Expleo's Global  
Cybersecurity  
Practice Leader



# Expleo's experts in this issue



**OLIVIER  
DE-VISSCHER**

Head of Railway  
Cybersecurity Centre



**JOHANNES  
AUGSTEN**

DE Head of  
CoC FuSi and Security



**RICHARD  
TEE**

UK Cybersecurity  
Practice Leader



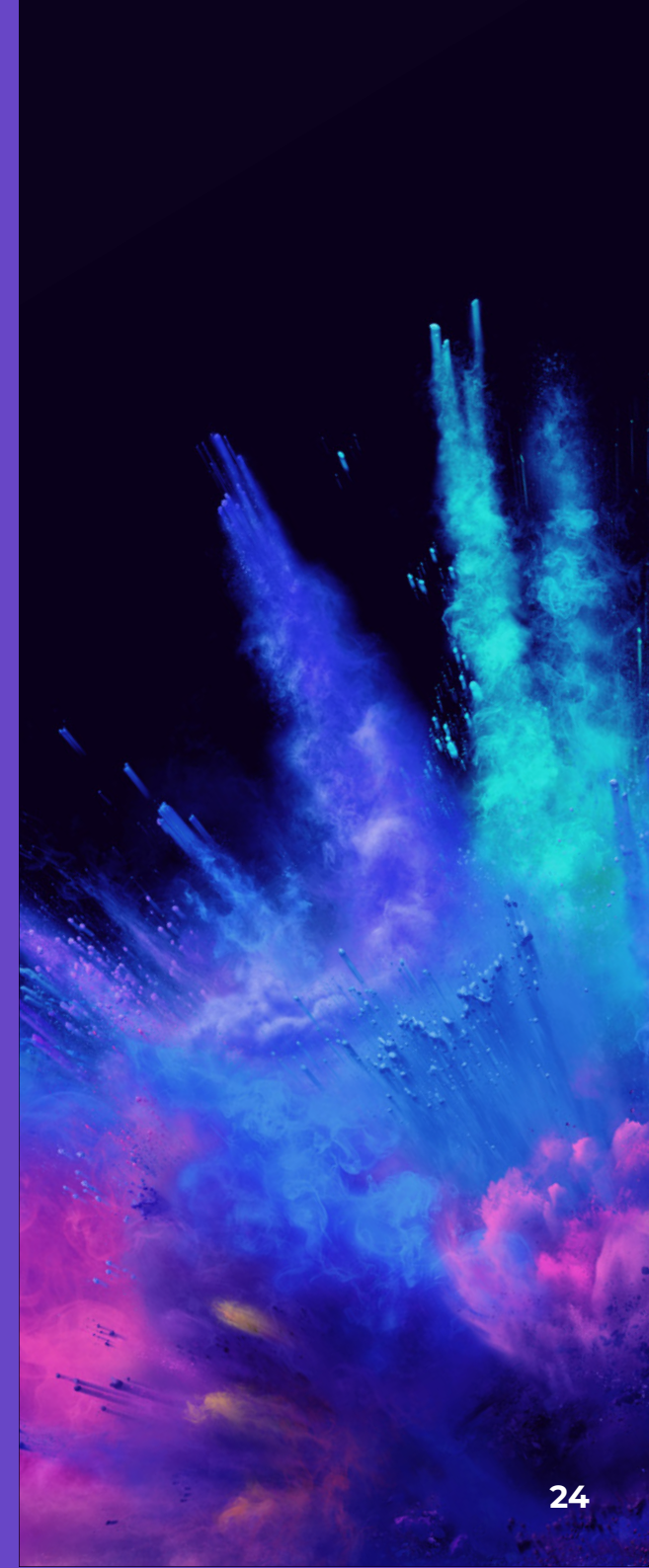
**FEDERICO  
SMITH**

Senior Cybersecurity  
Consultant



**YASMEEN  
TRIFISS**

Automotive  
Cybersecurity Engineer





## About Expleo

Expleo is a global engineering, technology and consulting service provider that partners with leading organisations to guide them through their business transformation, helping them achieve operational excellence and future-proof their businesses.

Expleo benefits from more than 40 years of experience developing complex products, optimising manufacturing processes, and ensuring the quality of information systems.

Leveraging its deep sector knowledge and wide-ranging expertise in fields including AI engineering, digitalisation, hyperautomation, cybersecurity and data science, the group's mission is to fast-track innovation through each step of the value chain.

As a responsible and diverse organisation, Expleo is committed to doing business with integrity and working towards a more sustainable and secure society.

Expleo boasts an extensive global footprint, powered by 15,000 highly-skilled experts delivering value in 30 countries and generating more than €1 billion in revenue.

**For more information,  
visit [expleo.com](https://expleo.com)**

[info@expleogroup.com](mailto:info@expleogroup.com)

[expleo.com](https://expleo.com)

**( expleo )**

Think bold, act reliable