Deloitte.

Automotive Cyber Security

Long-term Capability Building is Key to Protecting Vehicles, Business, and Customers

Executive Summary

Importance of Automotive Cyber Security

Automotive cyber security is crucial for protecting the safety and security of drivers, passengers, vehicles, and other assets like personal data. Besides physical safety reasons, the automotive industry may also be subject to legal and reputational consequences. But the increasing use of technology means automotive companies must be aware of potential risks and take appropriate measures.

Legal Framework

The European Union has adopted the UN-R 155 regulation as the legal framework for automotive cyber security. It requires automotive original equipment manufacturers (OEM) and suppliers to set up appropriate incident-response processes.

MAKING AN IMPACT THAT MATTERS since 1845

Importance of Incident-Response Exercises

As the pandemic has revealed, governments, companies, and individuals alike are unprepared for unforeseen emergencies. This can be largely avoided with regular exercises that are crucial to ensuring effective response to incidents. They help automotive companies build confidence, identify strengths and areas of optimization, improve (internal/external) coordination, increase awareness, and boost resilience.

Our Service Portfolio

We offer a comprehensive service portfolio for automotive clients to help them strengthen their management of incidents and achieve effective corporate resilience. This includes advising on creation of processes and organizational structure, on analysis and optimizing processes, and on conducting incident and emergency exercises. Our Continuous Capability Building Methodology is a valuable tool for organizations looking to enhance their incident-response and crisis-management capabilities.

Automotive cyber security is crucial to the industry and must be heeded by both automotive OEMs and suppliers. Adopting the UN-R 155 regulation and preparing for emergency situations through regular incident drills is essential for ensuring the safety and security of drivers, passengers, vehicles, and other assets. We are a strong and experienced partner that advises and supports automotive clients on effective incident and crisis management, as well as on corporate resilience.

Why Deloitte?

- Our automotive clients represent some of the world's largest OEMs, suppliers, dealers, captive finance companies, and aftermarket manufacturers
- Broad experience with, and insights derived from, implemented UNECE readiness programs and best practices as well as certified CSMS incl. type approvals
- Standardized and integrated assessment approach embedded in "Our Automotive Supplier Cyber Security Framework" considers current regulations and standards
- Global network of experienced auditors and automotive cyber security experts
- Standards organizations: Deloitte is member of DIN AK11 (ISO/SAE 21434, Cyber Security) and DIN AK12 (ISO/AWI 24089, SUMS)

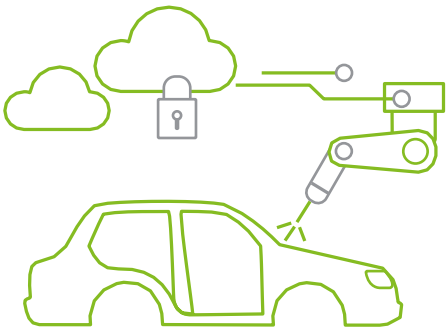
Main article

As the automotive industry continues to evolve, so does the threat of cyberattack. Increasing reliance on software and technologies has upped the need for robust cyber security measures in the automotive industry. This article explores the relevance of automotive cyber security, the legal framework for it, and the importance of cyber security in the automotive industry in the context of crisis management and corporate resilience, with a focus on incident response.

Why is Automotive Cyber Security relevant?

Risk assessments, reports, and our engagement with clients in recent years have shown a clear trend in cyber threats. The increasing number of diverse threats has a direct impact on the automotive industry and affects the production of cars in the shift towards e-mobility. ENISA reports that attacks target connected vehicle fleets and can cause catastrophic events.[3]

Rapid digitalization and the integration of advanced technologies into vehicles, including GPS, Bluetooth, Wi-Fi, cellular networks, and apps, has brought benefits to vehicle manufacturers and their customers alike. But these benefits also bring new security challenges because they can be exploited by malicious actors, resulting in theft, fraud, data-security breaches, and even physical safety risks. A single cyberattack, for instance, could simultaneously compromise hundreds of thousands of vehicles in a major risk to public safety, with damage even spreading to the source – the automotive client.



93%
of all automotive manufacturers have suffered a direct Cyber Security breach due to weaknesses in their supply chain, according to Forbes.[1]

66%
of attacks focus on supplier code, according to ENISA (2021).[2]

The automotive industry faces a variety of threats, including infotainment bugs, hacked paywalls and paid features or for physical security relevant cyberattacks on vehicles.

[1] Chuck Brooks, MORE Alarming Cybersecurity Stats For 2021 ! (sic), Forbes, 24. October 2021, accessed on 20. March 2023.
[2] European Union Agency for Cybersecurity, ENISA Threat Landscape For Supply Chain Attacks, July 2021, accessed on 20. March 2023.
[3] European Union Agency for Cybersecurity, ENISA Threat Landscape 2022, October 2022, accessed on 20. March 2023.

What is the legal framework for Automotive Cyber Security?
Adoption of United Nations Regulation No. 155 (UN-R 155/2021) by the European Union has created a set of requirements for automotive OEMs and suppliers to introduce and implement processes for incident response.

Automotive OEMs and suppliers must have processes in place to detect and respond to cyber security incidents. This includes having incident-response processes and plans, the capability to detect and report cyber security incidents, and ensuring that IT systems are secure. Automotive OEMs and suppliers should thus have an incident-response team, develop a communication strategy, and prepare employees for their roles and responsibilities with theoretical and practical training measures.

Which scenarios are most relevant?
Infotainment bugs, hacked paywalls and chargeable features, and high-impact vehicle cyberattacks are examples of the kinds of incident and crisis scenarios that threaten the automotive industry. In 2022, researchers managed to exploit vulnerabilities in connected cars and corporate platforms containing sensitive data.[4] They gained access to customer documents, manufacturer platforms, and internal company channels. More than 12 million vehicles worldwide are exposed to these and similar risks. The impact of a cyberattack can be severe for both vehicle drivers and OEMs. For drivers, cyberattack can result in theft, fraud, and safety risks. For OEMs, damage to brand reputation and the potential loss of customer trust can be devastating and long lasting. It can spread to relationships with investors, suppliers, and production networks, as well as to joint ventures for research and development purposes. Reductions in orders and sales are also conceivable. Moreover, OEMs may be liable for damages or compensation if a cyberattack results in harm to drivers, passengers, or surrounding environment (infrastructure and bystanders).

- **Infotainment Bugs**
  As vehicles become increasingly connected, the infotainment system has become a target for cyberattacks. Bugs can range from annoying glitches that affect the functionality of the system and distract drivers, to more serious security breaches compromising the privacy of driver and passenger.

- **Hacked Paywall or Chargeable Features**
  Another scenario is the hacking of paywall or chargeable features in the vehicle, allowing the attacker to access the system without paying and resulting in significant financial loss for the OEM.

- **Data Breaches**
  Cyber attackers can gain access to sensitive data stored in connected vehicles, such as personal and financial information, putting driver and passenger at risk of identity theft and other types of cybercrime.

- **High Impact Vehicle Cyber Attacks**
  The most serious type of attack impacts vehicle safety functions and can result in serious harm to driver, passengers, and bystanders. For example, a hacker could take control of the vehicle's braking system, accelerator or steering, putting the lives of individuals in danger and jeopardizing the safety of infrastructure.

The potential impact of cyberattack in the automotive industry is clearly far-reaching and serious. Automotive OEMs and suppliers must take proactive measures to protect against these threats and ensure the safety and security of their customers and vehicles.

Which services do we offer for Automotive OEMs and Suppliers?
As a strong and experienced partner in the automotive industry, we provide advisory services to help prepare for, and respond to, cyber security incidents. We understand that effective crisis and emergency management requires a holistic approach, involving all relevant stakeholders and a communication strategy for customers, suppliers, and the workforce.

Our services include advising on process creation and organizational structure, process analysis and optimization, and crisis or emergency exercises. We also provide theoretical and practical training measures to prepare management and employees for their roles and responsibilities within incident-response organization. We furthermore use targeted awareness measures to communicate the goals and requirements of vehicle security incident management to a wider group of employees.

Two essential elements for effective incident response are:

- **Regular emergency exercises,** where a simulated incident scenario is designed and carried out to test the preparedness and response capabilities of a company's incident-management team. Exercises are conducted in a controlled environment, allowing the team to practice their roles and responsibilities without risk of real-life consequences.

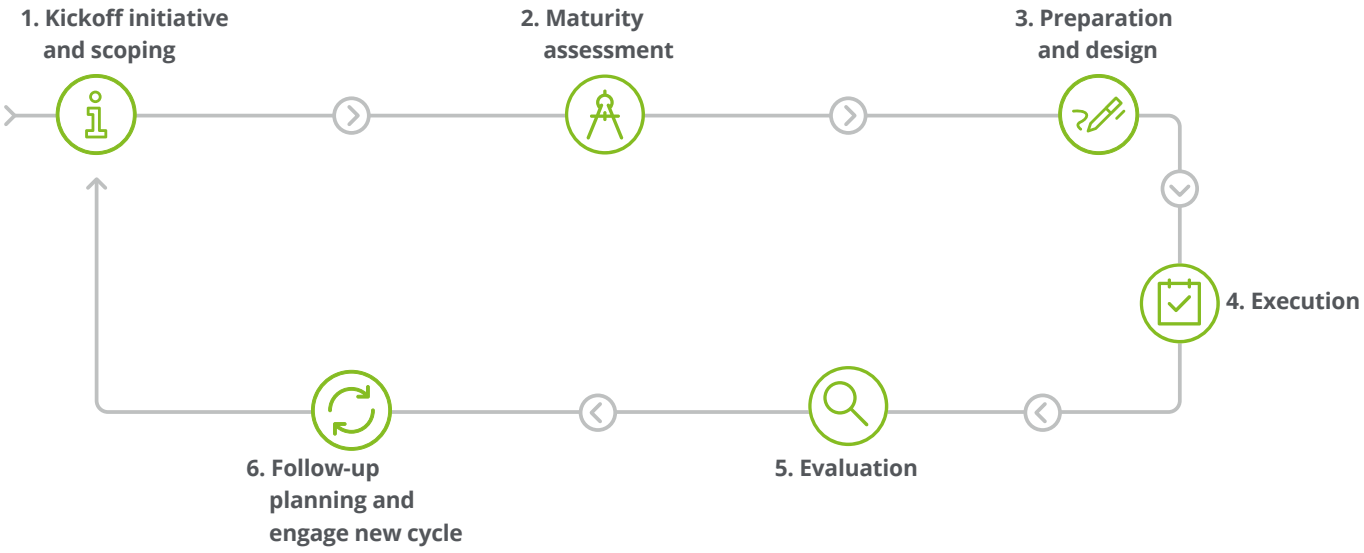
- **Collaboration between automotive OEMs and suppliers** is a growing trend to address the common challenge of cyber security. This includes sharing threat intelligence, best practices, and participating in joint incident-response exercises. It has also proven beneficial for aligning processes and enhancing cooperation at critical interfaces.

[4] Sam Curry, Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More, Blog, 03. January 2023, accessed on 20. March 2023.

How do we engage with our clients' challenges?
Together, we will develop a realistic scenario, based on the maturity level of the incident-response organization, to serve as the basis of the incident-management exercise. The objective is to develop a realistic and challenging scenario, to identify relevant exercise objectives and draft a corresponding script (including injects) that challenges the incident-response team without overwhelming it, and to derive optimization measures.

We have extensive experience in the development, execution, and analysis of incident scenarios. Scenarios are jointly developed to ensure a realistic story line and take into consideration the level of experience of participants with regard to existing plans, processes, and documentation. This maintains the quality of the exercise irrespective of training on the tactical or strategic level. The scenario will involve relevant stakeholders and external parties in different exercise domains as necessary to ensure realistic buildup and provide actionable learning.

Fig. 1 – Continuous capability-building cycle
Our methodology can be described as a continuous capability-building cycle:



1. Kickoff and scoping
- Establish joint understanding of exercise objectives, framework, participants, and stakeholders
- Presentation of the incident/crisis management organization, structures, and processes

2. If necessary: Maturity assessment
- Establish common understanding of the incident management framework and maturity
- Review of relevant documentation (e.g., processes)
- Interviews involving incident-management stakeholders
- Recommendations for exercises aimed at improving incident-response capabilities and organizational resilience
- Draft roadmap for long-term capability building (e.g., over the next three years)

3. Preparation and design
- Joint development and draft version of scenario, script, and injects
- Mapping of alerting structures, including crucial third-party providers along the supply chain
- Define exercise evaluation criteria based on assessed maturity level, exercise objectives, regulatory requirements, and best practices
- Preparation of media injects via the Deloitte CrisisSimulator and of briefing material for the exercise
- Define and socialize collaboration model (Deloitte's collaborative model is based on FORDEC, a method for structured decision making from the aviation industry)

4. Execution
- Our moderator and exercise coordinator(s) will closely monitor the reaction of the incident-response team and their effort in mastering the crisis
- The scenario will be escalated or de-escalated by using real time injects to ensure the appropriate exercise level for participants
- We recommend conducting the exercise jointly, with us leading the exercise through a dedicated moderator and support structure, supplemented with critical support from subject matter experts within your organization
- Initial feedback to and from participants.

5. Evaluation

- The exercise report follows a clear structure and serves as proof of functionality for incident-response and management procedures (if the exercise objectives are met)
- Based on established methods and best practices, we assess the exercise, analyze the results, outcomes, and evaluate participant performance
- Clear and concrete measures for improvement are derived from any identified gaps and findings
- Following review, feedback, and subsequent approval by relevant entities, the report is finalized

6. Follow-up planning

- Plan and draft roadmap for implementation of optimizing measures
- Review last exercise and optimization cycle and adapt project collaboration as necessary
- Review roadmap (if necessary) and define framework assumptions/guidelines for the next exercise
- Plan next kickoff and future work (according to roadmap)

Why are regular exercises critical for effective incident and crisis management?

Regular exercises and steady improvement of a company's incident-management capabilities are crucial for ensuring an effective response in the event of an emergency. Here are some of the key benefits of regular crisis-management exercises:

- **Build Confidence**
  By participating in regular emergency exercises, the organization and its employees develop routines and build confidence in their ability to respond effectively to emergency situations. Confidence in learned skills and established processes is essential to ensuring an effective response in the event of a crisis.
- **Identify Strengths and Areas of Optimization:**
  Regular emergency exercises provide an opportunity to identify and address optimization areas in crisis and incident-management processes or structures This information can be used to make improvements and ensure that the company is better prepared to respond to ever-changing crisis situations. The goal is sustainable, long-term, and continuous development of resilience capabilities.
- **Improve Coordination:**
  Regular training sessions help improve coordination among the various stakeholders involved in the response process, including employees, suppliers, customers, and regulators. This improved coordination is critical to ensuring an effective and efficient response to emergency situations.
- **Increase Awareness:**
  Regular incident- and crisis-management exercises increase awareness of the importance of crisis management and the role of everyone in the incident-response structure. This increased awareness is critical for ensuring rapid and effective response to an emergency.

Conclusion

Strengthening cyber security in the automotive industry is increasingly important as the branch evolves and is exposed to new potential threats. Appropriate measures and processes are essential to protect against cyberattack, safeguard brand reputation, and ensure customer safety.

Our Continuous Capability Building Methodology is a valuable tool for organizations looking to enhance their incident-response and crisis-management capabilities. By simulating an incident scenario in a controlled environment, organizations can test their response capabilities, identify areas for improvement, and make changes to continuously improve their incident-management processes. Companies become better prepared to respond to crisis situations, ensuring the safety and security of their customers and assets. We are well equipped to assist automotive OEMs and suppliers in achieving these objectives.

Bibliography

- Chuck Brooks, MORE Alarming Cybersecurity Stats For 2021 ! (sic), Forbes, 24. October 2021, accessed on 20. March 2023.
- European Union Agency for Cybersecurity, ENISA Threat Landscape 2022, October 2022, accessed on 20. March 2023.
- European Union Agency for Cybersecurity, ENISA Threat Landscape For Supply Chain Attacks, July 2021, accessed on 20. March 2023.
- Sam Curry, Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More, Blog, 03. January 2023, accessed on 20. March 2023.

Your Contacts

Michael Müller
Offering Lead Partner
Crisis & Resilience
Tel: +49 30 25468 5225
Mobile: +49 151 58000362
micmueller@deloitte.de

Ingo Dassow
Partner
Global Lead Automotive Cybersecurity
Tel: +49 30 25468 451
Mobile: +49 151 58001451
idassow@deloitte.de

Helge Wengerowski
Manager
Crisis & Resilience
Tel: +49 40 32080 4232
Mobile: +49 151 58000350
hwengerowski@deloitte.de

Deloitte.

Issue 04/2023