Automotive Cybersecurity Incident Response

Pocket Guide
Version 1.0

AQI | Automotive Quality Institute

Fraunhofer FOKUS

Preface

The automotive industry is facing new challenges due to innovative information and communication technologies and the increasing connectivity of vehicles. The security of vehicles and their protection against cyber attacks is crucial for the acceptance of these technologies and customer's safety. In addition to the cybersecurity aware development of these connected systems, the automotive industry must ensure a fast and effective response on cyber attacks in case of emergency. Therefore, a properly implemented process for an Automotive Cybersecurity Incident Response across the entire supply chain is required.

This pocket guide describes the necessary steps to build up such a process for an Automotive Cybersecurity Incident Response (Automotive CSIR). It provides checklists for its implementation and questions for an assessment of the Automotive CSIR readiness of a company. We hope that this guide helps managers as well as security experts to improve their Automotive CSIR capabilities. Any feedback to improve this pocket guide is welcome.

Content

The Automotive CSIR Process

Definitions

Automotive Cybersecurity Incident Response (Automotive CSIR)	is an application of the CSIR for automotive products and services, i.e. it applies to products installed in or connected with road vehicles and services used by vehicle users. (drivers, passengers, vehicle owners or fleet owners) The transition from the IT as a product or service for road vehicles to the enterprise IT is usually fluid. Each company must define the demarcation of Automotive CSIR to Enterprise CSIR appropriate to its organisation. Therefore, the concrete definition of automotive cybersecurity incident and thus Automotive CSIR may differ among companies.The goal of Automotive CSIR is the fast and effective respond to automotive cybersecurity incidents.
Automotive Cybersecurity Incident	is a single or series of unwanted or unexpected automotive cybersecurity events that have a significant probability of compromising road vehicles, related systems and services and threatening automotive cybersecurity.For the sake of brevity, the term cybersecurity incident is used in this guide to denote automotive cybersecurity incident.
Automotive Cybersecurity Event	is an identified occurrence of a system, service or network state indicating a possible breach of automotive cybersecurity policy or failure of controls, or a previously unknown situation that my be automotive cybersecurity relevant. It might turn out that an automotive cybersecurity event is a cybersecurity incident.For the sake of brevity, the term cybersecurity event is used in this guide to denote automotive cybersecurity event.
Vulnerability	is a weakness of an asset or control that can be exploited by one or more threats.
Threats	is a potential cause of an unwanted cybersecurity incident, which may result in a harm to road users.

The Core Activities of Automotive CSIR

The Automotive CSIR process consists of the following core activities, each cybersecurity incident runs through:

Detect & Register

First, a company must detect and register the cybersecurity incident. For this purpose, discovered cybersecurity events, reported vulnerabilities and newly identified threats are registered and forwarded to the responsible cybersecurity unit in the company.

Assess & Classify

After registration, a company must assess and classify the cybersecurity incident. The assessment consists of a technical and business impact analysis. After this phase, the cybersecurity incident is technically well understood and all information of a suitable response are available.

Decide & Response

Next, a company must decide which countermeasures to carry out and how to respond the cybersecurity incident. Although a respond can only be sustainable if the assessment of the cybersecurity incident is completed, some countermeasures should be initiated immediately, especially in case of emergency.

Learn & Optimize

Finally, a company should learn lessons from the cybersecurity incident and optimize its Automotive CSIR process. This phase of the process might trigger a sustainable product or service optimization, too.

In some organization parts of the activities might be covered by a vulnerability management process, which should be linked to the Automotive CSIR process.

Plan & Prepare

A company must **plan and prepare** the Automotive CSIR process.

According the German Federal Office for Information Security (BSI) this includes (IT-Grundschutz-Kataloge, 2016):

Establishing a method for dealing with cybersecurity incidents

Determining responsibilities in case of cybersecurity incidents

Determining reporting channels for cybersecurity incidents

Determining an escalation strategy for cybersecurity incidents

Determining of priorities for the treatment of cybersecurity incidents

Defining guidelines for the treatment of cybersecurity incidents

Defining cybersecurity incidents

A comprehensive guide on how to plan and prepare Automotive CSIR can be found from page NN.

The Automotive CSIR Team

(1/4)

It is recommended that a company of the automotive industry which offers cybersecurity relevant product, services or networks should have an **Automotive Cybersecurity Incident Response Team** *(Automotive CSIR Team)*.

This CSIR Team is responsible for the entire Automotive CSIR process and is the central unit for assessing and responding cybersecurity incidents in the company.

Depending on the company's size and organization, the Automotive CSIR Team can be a single person, how might involve experts from other units for each notified cybersecurity incident, a fixed cross-functional team having all required expertise, or something in between, i.e., a core CSIR Team extended by further experts for some cybersecurity incident types.

The Automotive CSIR Team

(2/4)

The Automotive CSIR Team should possess or should have access to the required know-how for a solid assessment and response of automotive cybersecurity incidents. This includes technical skills like:

- technical analysing of cybersecurity incidents
- assessing the technical impact of cybersecurity incidents
- finding vulnerabilities and software bugs
- closing vulnerabilities and fixing bugs

as well as organisational-legal expertise and knowledge like:

- assessing cybersecurity incidents regarding data protection acts, liability laws, financial and organisational aspects
- initiating non-technical measures like communication with authorities, customers and the public

The Automotive CSIR Team

(3/4)

For example, the following persons might join the Automotive CSIR team of an OEM:

Technical	Organizational-legal
System architect	Member of the committee for product safety
Component manager	Data protection officer
IT project manager / product owner	Member of the legal department
Application officer	Member of the HR department
	Member of the PR department

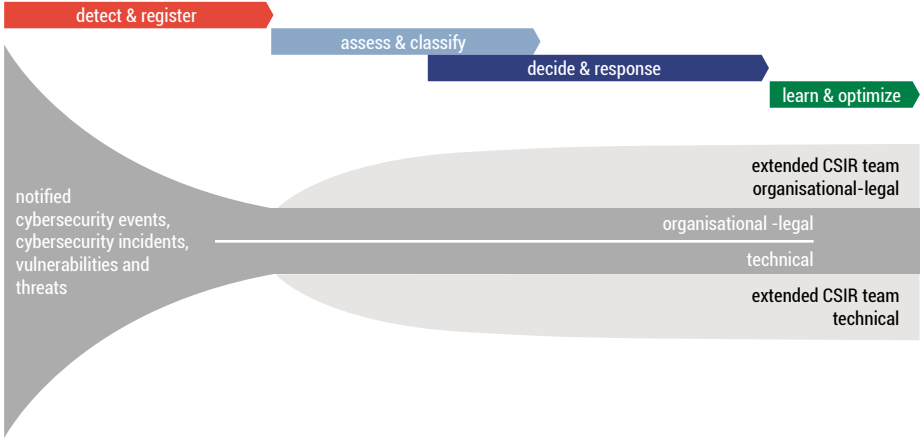
The Automotive CSIR Team

(4/4)

The majority of the detected cybersecurity events, cybersecurity incidents, discovered vulnerabilities and threats might not be reported directly to the Automotive CSIR Team. Instead, many of those issues might be reported to a support organisation, which forwards them in case of suspicion of a cybersecurity incident to the CSIR Team.

It is the CSIR Team that finishes the detect & register process by determining the occurrence of a cybersecurity incident. The CSIR Team might be extended by further experts during the cybersecurity incident processing according the type and criticality of the cybersecurity incident.

Core Activities



Process Reference Model & Process Performance Indicators for Automotive CSIR

In the following the core activities are described in more detail. For each process, there is an overview of this activity followed by a formal description according SPICE (ISO/IEC 33020:2015):

Process reference model	Process ID Process name Process purpose Process outcomes	The individual processes are described in terms of process name, process purpose, and process outcomes to define the process reference model. Additionally a process identifier is provided.
Process performance indicators	Base practices	A set of base practices for the process providing a definition of the tasks and activities needed to accomplish the process purpose and fulfill the process outcomes.
	Output work products	A number of output work products associated with each process.

While the process reference model defines the process and is essential, the process performance indicators are not obligatory and should be considered only as recommendations for the process implementation.

Detect & Register

(1/5)

The Automotive CSIR process starts with the detection and registration of cybersecurity events, cybersecurity incidents, vulnerabilities and threats.

This process includes:

Monitor systems and services

A cybersecurity event or incident targeting vehicles, vehicle-related software or a digital service is monitored and detected. This can be done e.g. by an intrusion detection system of the vehicle or server.

Monitor public information pools

A report of a vulnerability and threat is monitored and evaluated. Sources can be e.g. cybersecurity conferences or the darknet.

Accept and register incident

A cybersecurity event, cybersecurity incident, vulnerability or threat can be reported by external and internal sources e.g. customers, suppliers, authorities or dealers.

Assign and forward incident report

A notified cybersecurity event, cybersecurity incidents, vulnerability or threat is registered and forwarded to the internal unit(s) responsible for automotive security incidents.

Detect & Register

(2/5)

Process ID	CSIR.1
Process name	Detect and Register
Process purpose	Cybersecurity incident detection and registration aims to support the detection of cybersecurity incidents, cybersecurity events, vulnerabilities and threats. It provides means to receive, register, accept and forward cybersecurity incident reports from external and internal parties (support infrastructure).

Results of successful implementation of this process are as follows:

1. Information related to cybersecurity incidents is collected systematically.
2. Reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats are registered and documented.
3. Reports of cybersecurity events, cybersecurity incidents, vulnerabilities or threats events are classified so that responsibility is exposed.
4. Reports of cybersecurity events, cybersecurity incidents, vulnerabilities or threats are assigned for further processing.

Detect & Register

(3/5)

Base practices

CSIR.1.BP1 Monitor systems and services:	Check for cybersecurity events in systems and products. This activity aims for a systematic analysis of IT and product-related data that may show intrusion attempts, anomalies in usage, and suspicious network traffic. It is best supported with tools that allow collecting, centralizing, aggregating, and visualizing system monitoring data (such as SIEM tools) both in the field and in the IT infrastructure. [OUTCOME 1]
CSIR.1.BP2 Monitor public information pools:	Check for cybersecurity-related reports in public information pools, the press and other media. This activity consists of a systematic and periodic analysis of publicly available information on emerging threats, new vulnerabilities, and new attack capabilities that are related to the organization's services and products. This may be complemented by dedicated threat intelligence services and tools which actively push this kind of information into the organization. [OUTCOME 1]
CSIR.1.BP3 Accept and register incidents:	Accept and register cybersecurity events, cybersecurity incidents, vulnerabilities and threats. This activity requires the availability of dedicated contact points that are known publicly and inside the organization. The contact points shall be available 24/7 and allow for initial registration of reports related to cybersecurity events, cybersecurity incidents, vulnerabilities and threats. The registration process shall be able to document all incident- or event-related information as well as information on the reporter (such as their name, phone number, etc.) [OUTCOME 2]
CSIR.1.BP4 Assign and forward incident reports:	Assign reports on cybersecurity events, cybersecurity incidents, vulnerabilities and threats to internal entities that can further validate, assess and, if required, respond to the reported cybersecurity incident. [OUTCOME 3, 4]

Detect & Register

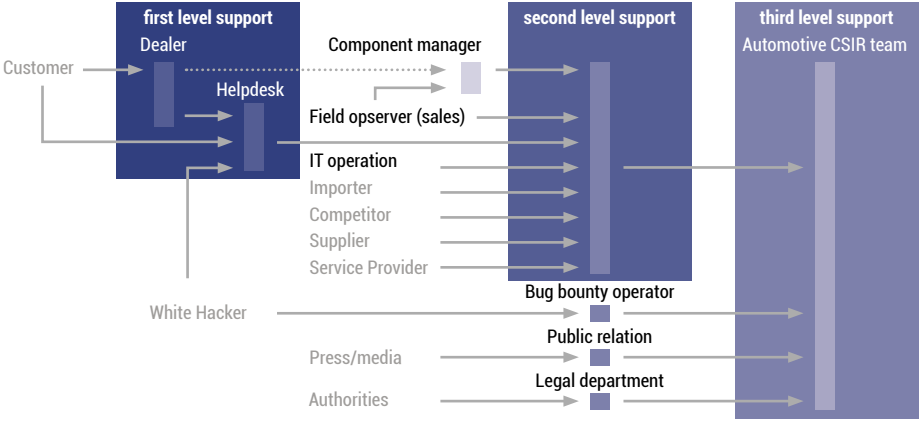
(4/5)

Output work products

Cybersecurity incident reports:	A cybersecurity incident report is the documentation of a disclosed cybersecurity incident. It contains information on the reporter (such as its name, contact details, etc.), the time (of registration and of observation), the reporter's observations of origin, effects and status, and any other information that is initially available. [OUTCOME 1, 2, 3, 4]

Detect & Register

(5/5)



Example of a support organization and an information work flow for detecting and registering automotive cybersecurity incidents at an OEM (italics: external reporters)

Assess & Classify

(1/4)

The Automotive CSIR team must assess the notified or discovered automotive cybersecurity incident – technically and organisational-legally. It must found and understood the cause of the cybersecurity incident and analyse the impact.

This process includes:

Analyse incident technically

The cybersecurity incident is technically analysed and assessed. The cybersecurity incident is well understood and the underlying vulnerabilities discovered.

Analyse risk

The business, safety, legal and operational impacts of cybersecurity incident are estimated and classified. Their risks for safety, data protection and functionality of the vehicles are assessed.

Inform internal stakeholders

Internal stakeholders are appropriately informed about the automotive cybersecurity incident.

Assess & Classify

(2/4)

Process ID	CSIR.2
Process name	Assess & Classify
Process purpose	Cybersecurity incident assessment & classification aims to validate cybersecurity incident reports, to assess cybersecurity incidents, and to identify the technical and organizational causes and impacts of cybersecurity incidents. This includes identification of vulnerabilities, assessment of the technical impacts and business, safety, legal and operational risks.

Results of successful implementation of this process are as follows:

1. The content of each cybersecurity incident report is validated.
2. The technical cause and impact of cybersecurity incidents are well understood.
3. The business, safety, legal and operational risks of cybersecurity incidents are well understood.
4. Internal stakeholders are informed.

Assess & Classify

(3/4)

Base practices

CSIR.2.BP1 Analyze incidents technically:	This activity aims to analyze and assess the technical cause and impact of incidents. Each cybersecurity incident report is initially validated and assessed on whether the report contains information on a critical cybersecurity incidents or whether the reported cybersecurity events require further investigation. If so, a full technical assessment of the incident is carried out. This includes a technical impact and a root cause analysis as well as the identification which products or services are affected. [OUTCOME 1,2]
CSIR.2.BP2 Analyze risks:	Analyze and assess the business, safety, legal and operational impacts and risks of the incidents. Business, safety, legal and operational risk assessment and management units should be involved. [OUTCOME 3]
CSIR.2.BP3 Inform internal stakeholders:	Distribute cybersecurity incident-related information to affected internal parties and stakeholders. [OUTCOME 4]

Assess & Classify

(4/4)

Output work products

1 Cybersecurity incident records:	A cybersecurity incident record is a record of all the details of a cybersecurity incident that documents the status of the incident response. It contains life cycle information starting with the initial detection and concluding with the resolution and closure of the cybersecurity incident. It may reference additional records related to the cybersecurity incident, such as cybersecurity incident reports, vulnerability records, forensic analysis, countermeasure documentation, etc. [OUTCOME 1]
2 Cybersecurity incident prioritization list:	This is a sorted list of cybersecurity incident records that organizes the order and schedule of assessment and response. [OUTCOME 1]
3 Assessment results:	This is the documentation of the cybersecurity incident assessment. It contains the results of the technical impact and risk analyses, information regarding causes and origin of the incident, as well as the business, safety, legal and operational impacts and risks of the incident. [OUTCOME 2,3]
4 Internal cybersecurity incident notifications:	This is a document about the cybersecurity incident and its importance for the organization that is appropriate for internal communication within the organization.Note: Depending on the target group, such a document may vary widely in its information content and its level of confidentiality. [OUTCOME 4]

Decide & Response

(1/4)

The Automotive CSIR team must decide which countermeasures should be carried out and how to response to the automotive cybersecurity incident. The countermeasures can be technical as well as organisational-legal.

This process includes:

Carry out immediate countermeasures

Immediate countermeasures are carried out in case of an emergency. Even if the cybersecurity incident might not be completely analysed, some cybersecurity incidents might require an instant respond.

Carry out sustained countermeasures

Sustained countermeasures are carried out, controlled and verified. The successful implementation of these countermeasures a required to finish this process.

Inform external stakeholder

Costumers, authorities and other stakeholders are properly informed and given instructions.

Preserve evidence

Evidence of origins, causes and effects of the automotive cybersecurity incident is preserved for further forensic investigations.

Decide & Response

(2/4)

Process ID	CSIR.3
Process name	Decide & Respond
Process purpose	Cybersecurity incident decision & response aims to ensure the confidentiality, integrity and availability of an organization's cyber-services and products by responding to cybersecurity incidents (including attacks and intrusions as well as other kinds of cybersecurity policy violations) to minimize the damage incurred by cybersecurity breaches.

Results of successful implementation of this process include the following:

1. Immediate actions are executed as required
2. Countermeasures are specified and agreed upon
3. Countermeasures are executed and monitored
4. Incidents are resolved
5. Proofs and evidence on origin, effects and course of a cybersecurity incidents are documented and archived
6. Users and stakeholders are informed as necessary

Decide & Response

(3/4)

Base practices

CSIR.3.BP1 Carry out immediate countermeasures:	If required, this activity executes immediate actions that are required to prevent and contain damage and preserve evidence in case of a critical or rapidly evolving threat. [OUTCOME 1]
CSIR.3.BP2 Carry out sustained countermeasures:	The aim of this activity is to define, decide, execute and monitor sustained countermeasures. This may include technical actions, such as software updates, new or changed cybersecurity configurations (such as firewall settings), application of custom configurations, creation of new accounts, and application of access controls. Since these measures are intended to restore products and systems to an operational, safe and secure state, appropriate testing and assurance of the product's and system's integrity and stability must be performed before rollout. Moreover, the countermeasures' effectiveness with respect to the identified threats must be assessed and validated after rollout. [OUTCOME 2, 3, 4]
CSIR.3.BP3 Preserve evidence:	Collect, preserve and archive forensic evidence that may be required to reject legal claims. [OUTCOME 5]
CSIR.3.BP4 Inform external stakeholders:	If required, users and other stakeholders are informed of the product or service failures as soon as possible. This process may involve distributing other information of importance to stakeholders, such as cybersecurity alerts. Effective customer service, including regular communication, ensures that external stakeholders are kept informed on the mitigation and recovery process. [OUTCOME 6]

Decide & Response

(4/4)

Output work products

1 Countermeasure documentation and status:	All implemented countermeasures are documented, including their rationales and decision and execution status. [OUTCOME 1, 2, 3, 4]
2 Forensic evidence records:	These data records store references to forensic artifacts, such as software images, memory dumps, log data, etc.Note: Storage of forensic data must satisfy specific requirements with respect to confidentiality, integrity and long-term safekeeping. [OUTCOME 5]
3 External cybersecurity incident notifications:	These are documents used to distribute information about the cybersecurity incidents and their importance to external stakeholders.Note: Depending on the target group, such documents may vary widely in their information content and confidentiality. [OUTCOME 6]

Learn & Optimize

(1/4)

After the automotive cybersecurity incident is resolved, the Automotive CSIR team should carry out a retrospective to capture the lessons learned and to optimize the CSIR process or trigger product improvements regarding cybersecurity.

This process includes:

Improve cybersecurity policies

Experiences from the incident resolution are used to fine tune the existing cybersecurity policy.

Improve product security

Findings from the incident resolution are used to optimize new products regarding cybersecurity.

Learn & Optimize

(2/4)

Process ID	CSIR.4
Process name	Learn & Optimize
Process purpose	The learn & optimize sub-process aims to identify potential improvements to processes and products in the aftermath of the cybersecurity incident handling process. The incident handling process is to be competed and closed by reviewing what initially occurred, what measures were implemented during detection and response, and how well the overall intervention worked. Learn & Optimize should be carried out after any major cybersecurity incident and periodically to cover lesser incidents.

Results of successful implementation of this process are as follows:

1. Process and policy improvements to the organization's cybersecurity policies, the cybersecurity incident response process, or related partner processes are identified and elaborated. Measures are specified and agreed upon.
2. Improvements to the affected products or systems are identified and elaborated.
3. Threat and vulnerability information is adapted according to new knowledge obtained by the cybersecurity incident handling process.

Learn & Optimize

(3/4)

Base practices

CSIR.4.BP1 Improve cybersecurity policies and processes:	Evaluate cybersecurity incidents and the cybersecurity incident handling process with respect to policy and process changes and identify concrete measures and procedures that require improvements to increase the efficiency and timeliness of the cybersecurity incident response process. This must include the identification of gaps in the qualifications or knowledge of personnel that could be remedied with training and education. [OUTCOME 1]
CSIR.4.BP2 Identify product improvements:	Identify concrete improvements that will help to make the affected systems more resilient against similar future cybersecurity incidents. This must include that development units and partners are sufficiently informed about vulnerabilities and that similar vulnerabilities in software variants and versions are addressed. This should include the identification of trends and patterns in threats and vulnerabilities and develop means to address them and may include participation in a community to exchange information on vulnerabilities, threats and incidents. [OUTCOME 2,3]

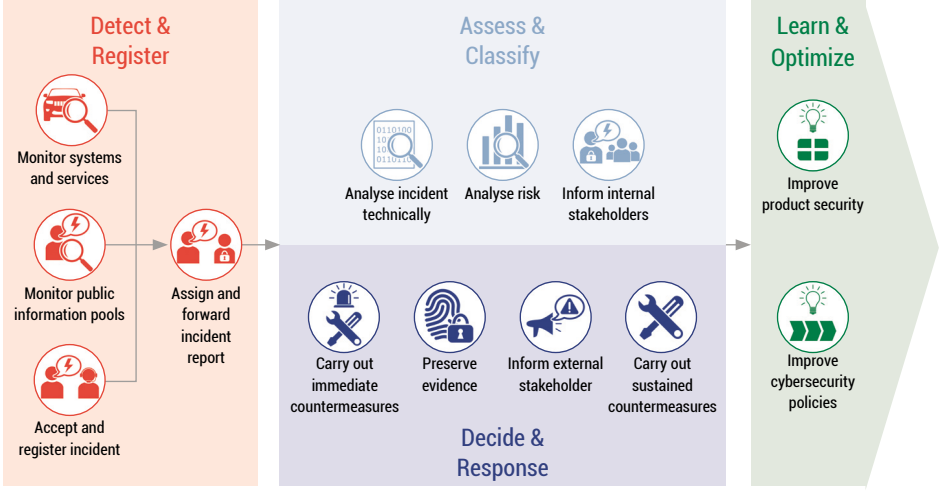
Learn & Optimize

(4/4)

Output work products

1 Cybersecurity policy:	A cybersecurity policy is a definition of rules and regulations that allows the secure operation of systems products and processes. [OUTCOME 1]
2 Process improvement reports:	A process improvement report includes a summary of instances in which the process has not performed as expected, suggestions for improvements to address the issues identified by the team to move towards a better process, and the action items that are chosen to prevent the recurrence of such instances. [OUTCOME 1]
3 Product improvement reports:	A product improvement report includes a summary of flaws, weaknesses, vulnerabilities and other cybersecurity-relevant findings in the organization's products, suggestions for product improvements, and the concrete action items chosen to address these findings. [OUTCOME 2]
4 Cybersecurity bulletins (i.e. updated vulnerability and threat information):	Cybersecurity bulletins include information for users, developers and partners to support and facilitate secure operation of the organization's products. [OUTCOME 3]

Summary of the Automotive CSIR Process



Automotive CSIR across the Supply Chain

(1/3)

In contrast to cases in which damage is caused by mechanical components, the vulnerabilities exploited in automotive cybersecurity incidents may be situated in IT components which are the responsibility of neither the OEM nor any of its suppliers or subcontractors. For example, vulnerabilities in the IT systems of the network operator or cybersecurity leaks from mobile devices that are connected to the vehicle may lead to automotive cybersecurity incidents. In the future, the attack surface of the road vehicle is likely to increase even further with more external IT systems, such as vehicle-to-infrastructure, vehicle-to-vehicle, vehicle-to-home, and other forms of vehicle networking. It may become necessary to involve the operators of these external IT components in the Automotive CSIR process as well.

The term **supplier** is still used here. However, this is not limited to suppliers of purchased parts that are installed in road vehicles or IT systems outside the road vehicle as part of the entire communication infrastructure; rather, it also includes the operators of digital services, which may lead to cybersecurity incidents.

Automotive CSIR across the Supply Chain

(2/3)

Within the Automotive CSIR process, suppliers essentially take on the role of development departments. In other words, suppliers cooperate closely with the Automotive CSIR technical team to analyze vulnerabilities identified in their systems and fix these vulnerabilities themselves. In addition, the suppliers carry out risk assessments regarding the identified vulnerabilities and inform any other customers similarly affected by them.

A supplier should also have a CSIR team, known to the OEM's Automotive CSIR team as a contact. The exchange of information between the OEM's technical Automotive CSIR team and the supplier's CSIR team in addressing a vulnerability is shown in the following table:

Automotive CSIR across the Supply Chain

(3/3)

No	Message	Content	Sender / Receiver
1	Reporting the cybersecurity incident	Description of the automotive cybersecurity incident Description of the assumed vulnerability	Customer to supplier
2	Acknowledgment of report	Designated contact Information about already available countermeasures (optional)	Supplier to customer
3	Acceptance criteria	Criteria for accepting a solution (possibly with message 1)	Customer to supplier
4	Analysis result	Confirmation of vulnerability, otherwise justified rejection Assessment result Information about forwarding to subcontractor (optional)	Supplier to customer
5	Measures	Description of measures carried out Information about acquisition of updates (if applicable) incl. system documentation	Supplier to customer
6a	Confirmation of acceptance	Confirmation if all acceptance criteria are fulfilled	Customer to supplier
6b	Rejection	Reasons for rejection if acceptance criteria are not fulfilled	Customer to supplier

Recommendations

Recommendations

Based on the foundation described in the first part, this second part recommends concrete activities for preparing and optimizing an automotive cybersecurity incident response.

These recommendations are intended for executives and employees of companies in the automotive industry who are directly or indirectly involved in the Automotive CSIR process or its preparation.

Recommendations to the upper management

Define basic cybersecurity policies and automotive cybersecurity incidents

The upper management should set the basic cybersecurity guidelines and define what the company considers to be an automotive cybersecurity incident. The basic cybersecurity guidelines should describe the secure and rule-compliant normal state when using vehicle IT so that an automotive cybersecurity incident may be identified as a violation of or deviation from this defined normal state. Based on these guidelines, an automotive cybersecurity incident can be distinguished from other incidents and events.

The definition should consider that existing organizational units are already processing incidents. Here it must be checked whether these existing organizational units are to be included in the automotive cybersecurity process or should work separately from the Automotive CSIR process.

Tasks

- [ ] Define basic automotive cybersecurity guidelines
- [ ] Define automotive cybersecurity incidents as distinct from other, non-vehicle-related cybersecurity incidents and other non-security incidents
- [ ] Communicate specifications

Recommendations to the upper management

Establish basic Automotive CSIR process and build up Automotive CSIR team

The upper management should describe the basic Automotive CSIR process, appoint an Automotive CSIR team, and instruct them in the structure and detailed definition of the process. Upper management should further equip the Automotive CSIR team with the necessary specialist competencies and/or organizational rights to enable it to perform technical and organizational-legal assessment of automotive cybersecurity incidents and to independently initiate countermeasures appropriate to the incidents' criticality and urgency in accordance with the cybersecurity guidelines for automotive cybersecurity incidents.

Tasks

- [ ] Define and communicate the basic Automotive CSIR process
- [ ] Build up an Automotive CSIR team and provide the necessary resources
- [ ] Define and communicate the decision-making rights of the Automotive CSIR team
- [ ] Establish guidelines for reporting to the upper management by the Automotive CSIR team
- [ ] Define and communicate the escalation process

Recommendations to the upper management

Build up or expand a support organization

The upper management should set up a support structure suitable for automotive cybersecurity incidents or adapt and expand the existing support structure for automotive cybersecurity incidents. Support might include the following:

- First-level support in the form of a publicly accessible help desk accessible via hotline, chat and/or e-mail, for example, and known to all external and in-house bodies
- Second-level support known and accessible to all component managers, field analysts, importers, suppliers, service providers, competitors, IT Operations and first-level support
- Third-level support known and accessible to second-level support, the bug bounty operator (if any), the PR department, and the legal department
- All support levels should be available 24 hours a day, 365 days a year. The support staff should have the necessary qualifications to detect and register automotive cybersecurity incidents and to carry out defined countermeasures.

Tasks

- [ ] Define support structures
- [ ] Provide resources for support structure and qualify employees
- [ ] Guarantee technical prerequisites for the availability of the support

Recommendations to the upper management

Prepare Automotive CSIR communication to external stakeholders

Upper management should define guidelines for communication with external stakeholders (including customers, authorities and the press) in case of automotive cybersecurity incidents. It should clarify what is to be communicated at what time by whom, so that all necessary information obligations are fulfilled, the necessary confidentiality is maintained, and efficient action is ensured.

Tasks

- [ ] Identify and document communication channels
- [ ] Define events that trigger external communications
- [ ] Clarify responsibilities for external communication

Recommendations to the upper management

Demand CSIR capability in the supply chain

Upper management should demand that suppliers of IT components provide a CSIR team and a CSIR process on the supplier side. This CSIR capability further implies that the supplier also requires this from its IT component suppliers, so that CSIR capability is present throughout the entire supply chain.

Tasks

- [ ] Define CSIR process guidelines for contracting IT component suppliers
- [ ] Communicate procurement guidelines
- [ ] Negotiate contracts with the IT component suppliers according to the guidelines and adjust them if necessary

Recommendations to the upper management

Test Automotive CSIR process (optional)

Upper management should have the Automotive CSIR process tested. For this purpose, critical incidents should be identified and described as test scenarios. When conducting a test, as few people as possible should be informed and it must be ensured that genuine damage is avoided. If necessary, external experts are t o be commissioned for this.

Tasks

- [ ] Identify critical cybersecurity incidents and define a test scenario
- [ ] Prepare the test to exclude the possibility of actual damage
- [ ] Carry out the test
- [ ] Identify the strengths and weaknesses of the Automotive CSIR process and remedy deficiencies

Recommendations to the upper management

Sensitize and train employees

The upper management should inform the employees of the company about the risks of cybersecurity threats and provide necessary training and support. The importance of automotive cybersecurity for the company should be clearly illustrated and employees should be sensitized to the subject. This applies especially to employees who may be involved in detecting automotive cybersecurity incidents or eliminating vulnerabilities.

Tasks

- [ ] Explain the importance of automotive cybersecurity for the company to the employees
- [ ] Offer training courses on cybersecurity in general and automotive cybersecurity in particular

Recommendations to the Automotive CSIR team

Specify cybersecurity policies

The Automotive CSIR team should substantiate and communicate the basic cybersecurity guidelines approved by the upper management. The concrete cybersecurity guidelines should contain guidelines for conduct regarding automotive cybersecurity incidents for the various groups or organizational units.

The support staff and the managers of IT components should be familiar with the following so that they can recognize automotive cybersecurity events at an early stage, assess them initially, and provide effective support in the further processing of automotive cybersecurity incidents:

- The secure normal state when using vehicle IT
- Possible automotive cybersecurity events
- Basic safeguards in case of a automotive cybersecurity incident
- Validated vulnerabilities, their detection, and countermeasures

Tasks

- [ ] Specify cybersecurity guidelines for automotive cybersecurity incidents and define guidelines for conduct for each group or organizational unit
- [ ] Document and classify automotive cybersecurity events
- [ ] Document validated vulnerabilities (detection and countermeasures)
- [ ] Communicate cybersecurity guidelines for automotive cybersecurity incidents

Recommendations to the Automotive CSIR team

Network with relevant experts and managers in the company

The Automotive CSIR team should know and be able to integrate at any time the experts and managers in the company necessary to assess automotive cybersecurity incidents, mitigate the damage, remove the causes of damage and/or restore the system. These may be employees of any of the following business units (among others):

- Data protection or legal department
- Product safety
- Component managers
- Human Resources
- Communication / PR
- Technical development and software development
- IT Operations

Tasks

- [ ] Identify all experts and managers relevant to the Automotive CSIR process
- [ ] Agree upon and define communication structure with experts and managers
- [ ] Ensure availability of experts and managers in emergencies
- [ ] Communicate cybersecurity policies deficiencies

Recommendations to the Automotive CSIR team

Access to compromised systems

The Automotive CSIR team should ensure in advance that it is permitted access to the compromised systems. For this purpose, organizational and technical framework conditions must be established.

Tasks

- [ ] Review and prepare legal, organizational and logistical options for accessing affected vehicles and vehicle components
- [ ] Organize access rights to IT systems for members of the Automotive CSIR team or have a facility secured in an emergency
- [ ] Set up any necessary access software for IT systems
- [ ] Seek instruction in the operation of the systems
- [ ] Access to log files and other relevant data

Recommendations to the Automotive CSIR team

Build up and use a network of external experts

The Automotive CSIR team should know external experts and, if necessary, consult them and be able to integrate them into automotive cybersecurity incident processing.

Tasks

- [ ] Identify external experts and build up and maintain a network
- [ ] Clarify contractual conditions and, if necessary, conclude contracts with external partners

Recommendations to the Automotive CSIR team

Ensure effective communication with external stakeholders

The Automotive CSIR team should ensure that any needed communication with external stakeholders' functions effectively. The stakeholders include the following (among others):

- Suppliers of IT components
- Authorities
- Competitors
- Customers (for subcontractors)

Tasks

- [ ] Know the contact persons at the external stakeholders
- [ ] Coordinate communication (triggering events, channels, data, data formats) with the external stakeholders and implement requirements
- [ ] Install or create and maintain processes, tools and templates for external communication

Recommendations to the Automotive CSIR team

Prepare risk assessment for automotive cybersecurity incidents

In coordination with the upper management, the Automotive CSIR team should establish a risk assessment procedure for automotive cybersecurity incidents and prepare templates for the procedure with examples.

Tasks

- [ ] Define risk assessment methods
- [ ] Define process for risk assessment
- [ ] Create templates with examples

65

Recommendations to the Automotive CSIR team

Document automotive cybersecurity incidents and secure forensic evidence

The Automotive CSIR team is to set up and operate systems for consistently documenting automotive cybersecurity incidents and forensic evidence (data and systems) as well as ensure professional processing of such evidence. The team must consider that the data collected must be kept confidential and stored for an extended period. The systems used must be designed for this purpose.

Tasks

- [ ] Define requirements for systems for documenting automotive cybersecurity incidents and preserving evidence
- [ ] Implement evidence preservation and documentation systems
- [ ] Seek training in the use of the systems for securing evidence and documentation
- [ ] Organizationally and technically ensure the confidentiality of the collected data
- [ ] Search for automotive cybersecurity incidents and connect or link automotive cybersecurity incident reports
- [ ] Determine the processing status of automotive cybersecurity incidents
- [ ] Build up and maintain expertise in forensic evidence preservation

Recommendations to the Automotive CSIR team

Ensure ability to validate effectiveness of countermeasures

The Automotive CSIR team should be able to verify the effectiveness of countermeasures. For this purpose, all necessary organizational and technical measures must be prepared.

Tasks

- [ ] Secure access to information about events in the field
- [ ] Be able to assess the information
- [ ] Ensure that automotive cybersecurity incidents are closed only by the Automotive CSIR team

Recommendations to the Automotive CSIR team

Gather automotive cybersecurity threats from external sources

The Automotive CSIR team should actively inform themselves about new automotive cybersecurity threats and, if necessary, integrate them into the Automotive CSIR process. Information sources include cybersecurity conferences and publications on cybersecurity, among others.

Tasks

- [ ] Screen sources and obtain information (for instance, by subscribing to newsletters, attending conferences, etc.)
- [ ] Install processes and tools for information gathering
- [ ] Evaluate external information about potential automotive cybersecurity threats and, if necessary, integrate it into the Automotive CSIR process

Recommendations to the Automotive CSIR team

Perform penetration tests (optional)

The Automotive CSIR team should be able to independently commission penetration tests to discover hitherto unknown vulnerabilities.

Tasks

- [ ] Know experts in penetration testing and be able to commission tests promptly if necessary
- [ ] If necessary, route the results of a penetration test into the Automotive CSIR process as an automotive cybersecurity incident

Recommendations to the Automotive CSIR team

Build up bug bounty platform (optional)

The Automotive CSIR team might build up a bug bounty platform that allows hackers to legally report vulnerabilities.

Tasks

- [ ] Develop a conceptual design (organizational, legal, financial, etc.) for building a bug bounty platform
- [ ] Operate the bug bounty platform

Recommendations to the Automotive CSIR team

Ensure capacity to disable critical features

The Automotive CSIR team should make it possible to switch off critical functions if necessary, provided the legal framework allows it.

Tasks

- [ ] Identify functions that should be capable of being disabled
- [ ] Describe the disabling mechanism for each of these functions
- [ ] Implement and test disabling mechanisms

Recommendations to component managers

Understand the significance of the component for automotive cybersecurity

The component manager should know the cybersecurity architecture and understand the significance of the component for which they are responsible. The component manager knows and has documented what data is stored in the component and what levels of confidentiality the data has.

Tasks

- [ ] Be familiar with cybersecurity guidelines
- [ ] Understand the significance of the component for automotive cybersecurity
- [ ] Know the data stored in the component and its level of confidentiality

Recommendations to component managers

Ensure ability to identify vehicles incorporating an affected component

The component manager should know which vehicles incorporate the component they are responsible for in order to be able to provide this information to the Automotive CSIR team for risk assessment.

Tasks

- [ ] Provide information about the vehicles with the component as needed in a timely manner

Recommendations to IT Operations

Log and monitor automotive cybersecurity events

IT Operations should be able to record automotive cybersecurity events in the vehicles and on the servers, to evaluate them initially and, if necessary, to initiate the Automotive CSIR process. For this purpose, the company should take the necessary preparatory steps.

Tasks

- [ ] Define and implement requirements for logging and monitoring of automotive cybersecurity events
- [ ] Ensure that IT Operations staff is automatically alerted to automotive cybersecurity events
- [ ] Build up and expand expertise in assessing automotive cybersecurity events

Recommendations to IT Operations

Ensure efficient deployment

IT Operations should enable efficient deployment of countermeasures to address automotive cybersecurity incidents by implementing the necessary technical and organizational requirements.

Tasks

- [ ] Ensure efficient verification of acceptance criteria
- [ ] Ensure efficient deployment of security patches
- [ ] Ensure efficient installation of security patches on the servers
- [ ] Ensure efficient distribution of security patches to customers and dealers

Evaluation of the Automotive CSIR Capability

Overview over Questions

The assessment of the Automotive CSIR capability consists of the following questions:

Detect & Register

To what extent can cybersecurity events and cybersecurity incidents targeting vehicles and vehicle-related software and digital services be monitored and detected?

To what extent are reports of vulnerabilities and threats monitored and evaluated?

To what extent can cybersecurity events, cybersecurity incidents, vulnerabilities and threats be reported?

To what extent are reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats correctly forwarded to the responsible internal unit(s)?

Assess & Classify

To what extent are cybersecurity incidents technically analyzed and assessed?

To what extent are the business, safety, legal and operational impacts of cybersecurity incidents assessed and classified?

To what extent are internal stakeholders appropriately informed about cybersecurity incidents?

Decide & Response

To what extent can immediate countermeasures be carried out in case of an emergency?

To what extent can affected customers, authorities and other stakeholders be properly informed and given instructions?

To what extent are sustained countermeasures carried out, controlled and verified?

To what extent is evidence of the origins, causes and effects of cybersecurity incidents preserved?

Learn & Optimize

To what extent are the findings and experiences from incident resolution used to optimize new products?

To what extent are the findings and experiences from incident resolution used to fine tune existing cybersecurity policies?

Capability to Detect & Register

(1/4)

To what extent can cybersecurity events and cybersecurity incidents targeting vehicles and vehicle-related software and digital services be monitored and detected (e.g., by log files, alerts, etc.)?

Objective

Monitoring and analysis of IT and product-related log and interaction data may show intrusion attempts, anomalies and suspicious network traffic and thus help to identify cybersecurity incidents and vulnerabilities.

Requirements

This must include:

- Awareness by organizational units other than dedicated incident response teams of the need to be on the lookout for cybersecurity events.
- Monitoring of cybersecurity events in our own products and services.
- Use of tools for cybersecurity event monitoring (e.g., SIEM tools) of backend systems.

This should include:

- Use of tools for cybersecurity event monitoring of vehicle systems and services (intrusion detection systems, product monitoring).
- Classification of products for cybersecurity reasons, in order to determine the type and scope of the monitoring.
- Defined processes, roles and responsibilities for the monitoring of cybersecurity events in vehicle systems and services (intrusion detection systems, product monitoring).

Capability to Detect & Register

(2/4)

To what extent are reports of vulnerabilities and threats monitored and evaluated (e.g., security conferences, darknet, scientific publications)?

Objective

Monitoring and analysis of public information pools may provide information on new attack capabilities, threats, recently discovered vulnerabilities and cybersecurity incidents, thus helping to identify vulnerabilities in our own products and services, as well as assessing the current threat landscape.

Requirements

This must include:

- Continuously monitoring suppliers' cybersecurity bulletins and public information pools on threats, vulnerabilities and cybersecurity incidents that are related to our own products and services.

This should include:

- Use of dedicated threat intelligence services and tools that actively feed these kinds of information into the organization.
- Continuous analysis of publicly available information (e.g., in the press and other media on cybersecurity incidents) about emerging new threats and new vulnerabilities that may relate to the organization's services and products.
- Defined processes, roles and responsibilities for the monitoring of suppliers' cybersecurity bulletins and public information pools.

Capability to Detect & Register

(3/4)

To what extent can cybersecurity events, cybersecurity incidents, vulnerabilities and threats be reported (e.g., by customers, suppliers, authorities, external cybersecurity experts, etc.)?

Objective

An organization must provide contact points so that external reporters can report cybersecurity events, cybersecurity incidents, vulnerabilities and threats that concern or are related to the products and services of the organization. These reports must be registered and processed to ensure the proper resolution of vulnerabilities and cybersecurity incidents.

Requirements

This must include:

- Contact details and/or methods for reporting cybersecurity events, cybersecurity incidents, vulnerabilities and threats that are available to external stakeholders (such as partners, customers and authorities).
- An internal organization that accepts and registers reported cybersecurity events, cybersecurity incidents, vulnerabilities and threats.
- Active management of reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats.

This should include:

Defined processes, roles and responsibilities to receive and register reported cybersecurity events, cybersecurity incidents, vulnerabilities and threats.

- The education of employees in the internal organization about automotive cybersecurity.
- Protecting the confidentiality and integrity of reports.

Additionally in case of high protection needs:

- Contact points with 24/7 availability.

Capability to Detect & Register

(4/4)

To what extent are reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats correctly forwarded to the responsible internal unit(s)?

Objective

The proper assignment of reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats to internal entities that can validate, assess and, if required, respond to these reports and ensure that they are handled properly and in a timely manner by the appropriate personnel in the correct order.

Requirements

This must include:

- The active assignment of reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats to internal

entities that can further validate, assess and, if required, respond to the reported cybersecurity events, cybersecurity incidents, vulnerabilities and threats.

- Awareness among service desk staff that critical systems may generate considerable damage in the event of ongoing vulnerabilities or cybersecurity incidents.
- Service desk checklists to support the identification of product-related cybersecurity events, cybersecurity incidents, vulnerabilities and threats.
- Labelling of reports when they are related to cybersecurity.
- Distribution of the definitions and policies related to automotive cybersecurity incident response among service desk staff and other units.
- Defined processes, roles and responsibilities to assess and classify reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats.

Capability to Detect & Register

(4/4 cont.)

This should include:

- Use of a ticket system that allows for assigning and managing responsibilities for cybersecurity events, cybersecurity incidents, vulnerabilities and threats.

This may include:

- Definition and distribution of dedicated escalation paths for reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats so that they can be handled differently from classical service requests and service disruptions.

Additionally in case of high protection needs:

- A dedicated automotive cybersecurity incident response team that is responsible for coordinating the product cybersecurity incident response and the addressing vulnerability issues for products in the field.

Capability to Access & Classify

(1/3)

To what extent are cybersecurity incidents technically analyzed and assessed (in regard to their cause, technical impact, etc.)?

Objective

The analysis, validation and classification of reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats must be performed by competent personnel. The analysis of the reports allows us to gain a technical understanding of their validity and criticality, the causes related to them and their technical impact. Validation and classification lead to a decision about whether reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats require an explicit

response, and thus whether they will be further addressed within the cybersecurity incident response process as a cybersecurity incident. Cybersecurity incidents must be properly prioritized so that effective countermeasures and immediate actions can be promptly and appropriately initiated in accordance with the criticality of the security incident. The early and proper analysis and preservation of the causes of the incident (forensics) can help to answer liability questions which may arise in the aftermath of a cybersecurity incident.

Requirements

This must include:

- Classification of reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats in respect to their validity and criticality, as a basis for further investigation and treatment.

  – A classification scheme to support decision-making about trustworthiness and criticality, vulnerability and cybersecurity incident reports.

Capability to Access & Classify

(1/3 cont.)

- A technical and organizational means of searching for reports that have similarities (e.g., similar cybersecurity events, cybersecurity incidents, vulnerabilities or threats).

- Defined processes, roles and responsibilities concerning the making of decisions about whether reports of cybersecurity events, cybersecurity incidents, vulnerabilities and threats need further treatment and for managing and coordinating the related security incident response activities.

- Root cause analysis and impact analysis for cybersecurity incidents

- Dedicated processes to analyze and assess the root cause of cybersecurity incidents

- Dedicated processes to analyze and assess the technical impacts of cybersecurity incidents

- Defined processes, roles and responsibilities that establish contact channels to technical staff who can provide details about each of the organization's relevant products and services.

- Defined processes, roles and responsibilities that establish the interaction between the automotive cybersecurity incident response team and the risk assessment units.

- Documentation (i.e., creation of an incident record) and prioritization of cybersecurity incidents in terms of their criticality, as a basis for treatment measures and immediate actions.

This should include:
- Access to forensics services that allow for the systematic assessment of compromised systems and safekeeping of clues, traces, logging data and other forms of evidence.

- Dedicated processes for technical cybersecurity risk assessment and management.

- Contact channels to responsible roles and units in the supply chain.

This may include:
- Defined processes, roles and responsibilities that enable the secure preservation of data from suspicious systems in a verifiable manner.

Additionally in case of high protection needs:
- An automotive cybersecurity incident response team with dedicated forensics know-how.

Capability to Access & Classify

(2/3)

To what extent are the business, safety, legal and operational impacts of cybersecurity incidents assessed and classified?

Objective

The analysis of business, safety, legal and operational impacts and risks supports the definition of adequate countermeasures and may initiate activities in supporting processes like public relations, legal, human resources, etc.

Requirements

This must include:

- Analysis and assessment of the business, safety, legal and operational risks of a cybersecurity incident.

This should include:

- Involvement of the business, safety, legal and operational risk assessment and management units.

Capability to Access & Classify

(3/3)

To what extent are internal stakeholders appropriately informed about cybersecurity incidents?

Objective

Internal stakeholders (e.g., management, public relations, human resources and the relevant technical departments) need to be informed about the origin, effects and progression of a cybersecurity incident, so that they can be involved in the determination of immediate actions and systematic countermeasures.

Requirements

This must include:

- Distribution of information about the occurrence of cybersecurity incidents to affected internal parties and stakeholders.
- Distribution of status information related to the incident response to affected internal stakeholders.

This should include:

- The existence of pertinent and appropriate templates for reports that provide information suitable for internal stakeholders.

Capability to Decide & Response

(1/4)

To what extent can immediate countermeasures be carried out in case of an emergency?

Objective

Immediate actions are required to contain damage and preserve evidence in cases in which the threat is rapidly evolving.

Requirements

This must include:

- Defined processes, roles and responsibilities for initiating and managing immediate response actions.

This should include:

- Dedicated policies for handling ongoing cybersecurity incidents and severe vulnerabilities in the field.
- Direct contact to the responsible roles and units in the supply chain.

Additionally in case of high protection needs:

- 24/7 availability of personnel that are needed to carry out immediate response actions (e.g., external communications, informing the press, deactivating systems, ...).

Capability to Decide & Response

(2/4)

To what extent can affected customers, authorities and other stakeholders be properly informed and given instructions?

Objective

Users and other external stakeholders (e.g., business partners, public authorities) need to be involved in order to mitigate the impact of a cybersecurity incident and to fulfill legal obligations.

Requirements

This must include:

- Informing users and other stakeholders about product or service failures as soon as possible, if required.

- Policies to ensure that all affected or relevant external stakeholders are promptly informed about the occurrence of a cybersecurity incident and the mitigation and recovery processes related to it.
- Dedicated channels of communication to all affected or relevant external stakeholders who are required to be promptly informed in case of a cybersecurity incident (e.g., an effective customer service system that includes regular communications with external stakeholders and users).
- Policies to ensure that no unauthorized person has access to information about the cybersecurity incident.
- Direct contact to the responsible roles and units in the supply chain.

Capability to Decide & Response

(3/4)

To what extent are sustained countermeasures carried out, controlled and verified?

Objective

The proper execution and verification of countermeasures to eliminate the cause of a cybersecurity incident, mitigate its consequences and initiate the associated changes to the product or service is essential to incident reaction and prevention.

Requirements

This must include:

- Policies to ensure that countermeasures are properly defined and decided upon.
- Management structures to decide upon the countermeasures to be taken.

- Organizational roles and units that can execute and control countermeasures, with the aim of returning to an operational, safe and secure state in products and systems.
  - Appropriate testing, confirmation and assurance of the product's and system's integrity and stability before rollout.
  - Appropriate assessment and validation of countermeasure effectiveness with respect to identified threats after rollout.

This should include:

- A regularly maintained list of customizable countermeasures and standard responses.
- Continuous monitoring of the status of efforts to address unresolved cybersecurity incidents, so that additional countermeasures may be introduced as soon as possible if threats are improperly addressed or if service levels are likely to be breached.

Capability to Decide & Response

(4/4)

To what extent is evidence of the origins, causes and effects of cybersecurity incidents preserved?

Objective

After a cybersecurity incident has occurred, evidence must be handled with precision and care to prevent it from being overwritten, destroyed or otherwise corrupted, so as to improve assessment outcomes and reduce the potential for lawsuits or fines.

Requirements

This must include:

- Ensuring that countermeasures are executed in their entirety and collecting, preserving and archiving forensic evidence that may be needed to reject legal claims.
- A technical infrastructure to preserve and archive forensic evidence that may be needed to reject legal claims.
- Policies to ensure that forensic evidence is confidentially stored..

Capability to Learn & Optimize
(1/2)

To what extent are the findings and experiences from incident resolution used to optimize new products?

Objective

Experiences and insights from the Automotive Cybersecurity Incident Response process shall be used to improve cybersecurity measures in new products over the long term. To this end, these experiences and insights must be systematically prepared, consolidated and disseminated to all relevant organizational units.

Requirements

This must include:

- The identification of improvements that would make the affected systems more resilient against existing or future threats, vulnerabilities and cybersecurity incidents, or the same or similar ones.

- Providing information to development units and development partners about vulnerabilities and other technical causes of a cybersecurity incident.
- Ensuring that development units and development partners sufficiently address these vulnerabilities.
- Ensuring that similar vulnerabilities in different software variants and versions are addressed.
- Deriving long-term cybersecurity measures from information about cybersecurity incidents and sending these measures to technical development.

This should include:

- The identification of trends and patterns with respect to threats and vulnerabilities and the means to address and manage new patterns.
- The evaluation of cybersecurity incidents so that new threat information can be identified and the provision of this information to technical development.

This may include:

- Participation in a community which exchanges information on vulnerabilities, threats and cybersecurity incidents.

Capability to Learn & Optimize

(2/2)

To what extent are the findings and experiences from incident resolution used to fine tune existing cybersecurity policies?

Objective

Experiences and insights from the Automotive Cybersecurity Incident Response process shall be used to improve cybersecurity measures in the organization. To this end, these experiences and insights must be systematically prepared, consolidated and disseminated to all relevant organizational units.

Requirements

This must include:

- The identification of gaps in personnel qualifications that could be resolved by training and education.
- A dedicated vulnerability management process.

This should include:

- Deriving new patterns to be used for the detection of cybersecurity incidents from most recent information about cybersecurity incidents and the provision of this information to the organizational units that are responsible for incident detection.

Authors

Gunnar Harde
(AQI Automotive Quality Institute GmbH)

Dr. Jürgen Großmann
(Fraunhofer-Institut FOKUS)

Contact

AQI Automotive Quality Institute GmbH
Französische Str 13-14
10117 Berlin
Germany

kontakt@aqigmbh.de

www.aqigmbh.de

This publication is based on the expertise of the AQI and its scientific partners. It represents a consolidated position on the topic under examination.

This work including all its parts is protected by copyright. Any use not expressly authorized by copyright law requires prior permission.