Study on Incident Response System of Automotive Cybersecurity

Yanan Zhang, Peiji Shi(✉), Yangyang Liu, Shengqiang Han,
Baoying Mu, and Jia Zheng

China Automotive Technology and Research Center Co. Ltd.,
Tianjin 300393, China
spj_2004@126.com

Abstract. With the development of Intelligent Connected Vehicles, a large number of automobile cybersecurity incidents also occur. Scientific and reasonable incident response system is the key technology to ensure the successful handling of cybersecurity incidents. From the point of view of management, referring to the construction of incident response system in IT industry and combining with the characteristics of automobile cybersecurity, this paper puts forward the framework of incident response system for automobile cybersecurity. The framework includes five aspects: plan and prepare, detection and reporting, assessment and decision, responses and lessons learnt. Emphasis is laid on the formulation and updating of management policy, the establishment of incident response team, incident coordination mechanism and so on. Then, based on the method of questionnaire survey, the evaluation method of incident response capability is put forward. The research method makes up for the blank of automobile industry in cybersecurity incident response, and has an important positive role in reducing the adverse impact of security incidents.

Keywords: Automotive cybersecurity · Incident response · Evaluation system · Questionnaire

1 System Framework

In the traditional field, establishing an incident response system is one of the effective security services for solving network system security problems. The incident response system in the traditional field includes the incident response system for enterprises' production safety accidents, the incident response system for public disasters and accidents, and the incident response system for traditional public health safety incidents, etc. [1, 2]. The corresponding laws and regulations and related work technologies have been established in various fields, and certain technological innovation. The event response methodology is the discipline that studies the event response process. The event response method is not unique. It is widely accepted that the PDCERF methodology is the earliest classical method, which divides the corresponding process into six stages of preparation, detection, containment, eradication, recovery and Follow-up [3, 4]. But in this process, there is no clear distinction between the tasks of the victim and the responder. The NIST.SP.800-61r2-computer security incident

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 198–209, 2019.
https://doi.org/10.1007/978-3-030-21373-2_16

handling guide in the United States divides the incident response into four steps: Preparation, detection & Analysis, Containment Eradication & Recovery, and Post-incident Activity four stages. ISO 27035 divides incident response into five steps: plan and prepare, detection and reporting, assessment and decision, incident responses, and lessons learnt [5, 6]. This paper will establish an automotive cybersecurity incident response system according to the idea of 27035.

2 Plan and Prepare

2.1 Development and Update of Management Policy

The organization's cybersecurity incident management policy should provide the principles and intent of formal records to guide decisions and ensure consistent and appropriate implementation of processes, procedures, etc. related to this policy. Any cybersecurity event management policy should be part of the organization's cybersecurity policy. It should also support the existing mission of its parent organization and be in line with existing policies and procedures. Before making a cybersecurity policy, the organization should consider the purpose, internal and external related groups, the types of events and vulnerabilities that require special attention, and the need for specific personnel, the benefits to the entire organization or department, etc. The management policy should be high-level and applicable to all employees and contractors. Details and steps should be included in a series of documents.

2.2 Develop a Management Plan

The management plan document should include multiple documents, including forms, procedures, event classification, organizational elements, and support tools for testing and reporting, evaluating and making decisions, responding to and learning from cybersecurity incidents. The management plan includes a basic low-level and high-level summary of incident management activities to provide the structure and pointers to the detailed components of the plan. These components provide step-by-step instructions for event handlers to work with specific tools, follow specific workflows, or handle specific event types as appropriate.

2.3 Establish Incident Response Team (IRT)

The purpose of establishing a cybersecurity incident response mechanism is to provide organizations with the appropriate capabilities to evaluate, respond to, and learn about cybersecurity incidents and provide the necessary coordination, management, feedback, and communication. IRT helps reduce physical and monetary losses and reduces the damage to the organization's reputation that is sometimes associated with cybersecurity incidents.

IRTs can be structured differently based on the size of the organizational, employee and industry type.

Effective event response depends on the capabilities and reliability of the IRT staff.

The IRT should be responsible for ensuring that the incident is resolved. In this case, the IRT manager and team members should have the authority to take the necessary actions and consider it appropriate to respond to cybersecurity incidents. However, actions that may adversely affect the entire organization, whether financially or reputational, should be approved by top management. Therefore, cybersecurity incident management policies and plans must detail the appropriate authority for the IRT manager to report serious cybersecurity incidents to them. The authority shall undertake to provide services to IRT members and provide timely guidance.

2.4 Communication with Other Organizations

Incident management is not a self-contained process. Relationships, communication channels, data sharing agreements, and policies and processes should be established throughout the organization. These internal collaborations may include coordination with business managers, IT representatives, human resources representatives, public relations representatives, any existing security groups, any law enforcement liaisons, or investigators. The organization should also establish a relationship between the IRT and the appropriate external stakeholders.

2.5 Technical Support

To ensure a prompt and effective response to cybersecurity incidents, the organization shall acquire, prepare and test all necessary technical and other support means. All internal and external parties to support and reporting should have a clear definition and agree on communication channels and workflow.

2.6 Cultivate Safety Awareness and Strengthen Drills

Cybersecurity incident management is a process involving both technical means and people. Therefore, it should be supported by individuals with appropriate cybersecurity awareness and trained individuals within the organization.

2.7 Incident Management Plan Test

The organizations should regularly review and test cybersecurity incident management processes and procedures to highlight potential defects and problems that may arise when managing cybersecurity incidents and vulnerabilities. Regular tests should be organized to check the process/procedure and verify the IRT response.

2.8 Summary and Improvement

Once the cybersecurity incident is over, it is important that the organization quickly identify and learn lessons from the cybersecurity incidents and ensure that the conclusions are implemented. In addition, lessons can be learned from assessing and resolving reported cybersecurity vulnerabilities.

3 Detection and Reporting

The detection and reporting stage mainly involve the collection, recording, and reporting information related to security events [7]. Its key activities include monitoring the recording system and network activities, detecting and reporting discovered security events or security vulnerabilities, collecting security events or security vulnerability information and events development trends. At this stage, it has not been determined whether a cybersecurity event has occurred. It should ensure that all activities, results and decisions are fully and completely documented for future analysis and improvement, while ensuring the secure collection and storage of relevant electronic evidence.

In the detection and reporting stage, the change control mechanism should be followed to continuously track cybersecurity events and vulnerabilities. All information should be stored in the cybersecurity database in a timely and complete manner and kept up-to-date, and system upgrades should be performed as needed for further evaluation, decision, review or take action.

4 Evaluation and Decision

Based on the security problems or security vulnerabilities detected in the previous stage, the relevant information is collected, tested and processed, and the special evaluation agency evaluates whether it is a cybersecurity incident [8]. If the false alarm is suspected, the IRT can conduct quality review to ensure that the incident processing procedure is correct.

Once identified as a cybersecurity incident, the responsibility of the responders should be defined immediately according to the corresponding distribution system.

Issue formal guidance documents and decision documents, including review and modification of reports, evaluation results, internal notices, etc., and comprehensively recording security incident information and follow-up activities according to the guidelines.

This stage should ensure that all relevant parties involved in the IRT focus on all activities, results and decisions are correctly and completely documented for future analysis. At the same time, ensure that the change control mechanism is maintained to cover cybersecurity event tracking and event reporting updates, and to keep the cybersecurity database up to date [9].

5 Incident Response

According to the evaluation and decision results, the responders can make incident response quickly. The response steps are as follows:

Conduct security event classification. The classification of cybersecurity events mainly considers the importance of information systems, system losses and social impacts [10, 11]. It can be divided into extraordinary major events, major events, larger events and general events, as shown in Table 1 [12].

Table 1. Cybersecurity event classification.

Level	Loss of information systems			Social influence
	Particularly important information system	Important information system	General information system	
Extraordinary major events (Class I)	Especially serious	——	——	Extraordinary major
Major events (Class II)	Serious	Extraordinary serious	——	Major
Larger events (Class III)	Larger	Serious	Extraordinary serious	Larger
General events (Class IV)	Smaller	Larger	Serious or below	General

The IRT review determines whether the cybersecurity event is under control. If the event is controllable, the required response will be executed. If the event is uncontrollable or will have a serious impact on the organization's operations, the incident response is implemented by upgrading to the incident management function [13].

Allocate internal resources and identify external resources in response to events.

After recovering from an accident, the post-incident actions should be initiated based on the nature and severity of the incident, including investigating information related to the incident, investigating relevant personnel and other relevant sources, and the summary of the investigation result report [14].

After the security incident is resolved, it should be closed according to the requirements of the IRT or the parent organization and notify all stakeholders.

Based on IRT communication planning and information disclosure policy, to the asset owner and can help manage and solve the problem of internal and external organizations (such as other incident response teams, law enforcement agencies, Internet service providers, and information sharing organizations) to share information, provide the existence of security incidents, threats, attacks and vulnerabilities and other information.

In addition, actions such as record and report updates, cybersecurity database updates, and forensic data collection and storage should be carried out throughout this stage [15, 16].

6 Lessons Learnt

After the security incident is resolved, it should be reviewed and summarized to draw lessons. Key activities in the stage include:

Summarize the control implementation management policy, cybersecurity risk assessment and management review system related to improving automotive cybersecurity;

Evaluate and optimize the response process, report format, organizational structure, etc.;

Review the effectiveness of incident response, improve cybersecurity incident plans and management plans, and evaluate regularly.

Sharing the results of the review with the public and share and communicating with other incident response teams to improve their incident response capabilities for similar problems [17].

7 System Evaluation

The fundamental purpose of automotive cybersecurity incident response is to detect the type of attack in time and minimize the scope of the loss. However, the cybersecurity threats faced by different automobile companies and different models at different stages of development vary greatly. Therefore, how to establish a universal automobile cybersecurity incident response system, and provide reference for the formulation of incident response contingency plan and management formulation is the key problem to be solved in this paper.

7.1 Review Metrics

Based on the whole life cycle of the vehicle, considering the main objectives of each stage of the incident response, the six factors of management system, organization, personnel level, emergency materials and facilities, technology and treatment methods, records and reports are selected as key elements in the evaluation of automobile cybersecurity.

7.2 Review Questionnaires

Based on the framework of the automotive cybersecurity incident response system, the design review questions for the review of key elements are presented around Sect. 4. Considering the universality of the questionnaire, consider the issue of setting multiple levels for each element, and each part can be answered separately. The problem is mainly in the form of multiple-choice questions. For the question with the answer “yes”, there are some extension problems in the form of blank-filling question [18].

In order to simplify the answer form of the review questionnaire and reduce the error caused by the subjective factors of the respondents, the answer to the multiple-choice questions is designed to include three options, namely “yes”, “no” and “partial”. The answer to the blank-filling question is open, and the user answers it according to his or her own situation.

The contents of the questionnaires at each stage are as follows:

Plan and prepare stage (1) In terms of management system, the review management policy is formulated and updated. Does the management plan include formalities, procedures, event classification, organizational elements, support tools, testing and other elements, and IRT managers’ report serious cybersecurity to top management?

(2) In terms of organization, the authority will assess whether an IRT has been established, its structural form, through a collaborative mechanism with business managers, its representatives, human resources representatives, public relations representatives, any existing security groups, any law enforcement liaison officers or investigators, whether the bureau provides services and guidance to IRT members. (3) In terms of technology and processing capabilities, whether to acquire, prepare and test the necessary technologies and other supporting means. (4) In terms of personnel level, the frequency and form of training exercises, and whether the organization has the appropriate cybersecurity awareness and the support of trained individuals. (5) In terms of records and reports, whether detailed information and procedures for the development and updating of the management system are recorded, and whether there are records of summary and improvement after the completion of the security incident.

Detection and reporting stage (1) In terms of management system, the main focus is on the monitoring system, that is, whether the automobile and related services, back-end systems, vehicle systems and public information database are actively monitored. If monitoring measures have been taken, the monitoring tools and technical means will be further investigated. (2) In terms of personnel level, it involves the review of the level of incident response team members and non-incident response team personnel, respectively, to assess their awareness of the importance of incident response, whether they can clearly define security events, and whether they know the contact person and contact information of security events. In addition, attention should also be paid to the training and application of the professional ability of the incident response team members to receive training drills and timely safety event marking. Also focus on whether stakeholders are aware of security event contacts and contact information. (3) In terms of technology and processing mode, attention is paid to the difference between security issues and security incidents for service requests and service interruptions. (4) In terms of organizational structure, it is concerned with whether or not to set up a special institution to register security incidents. Whether the institution is responsible for formulating, preserving, updating and monitoring the test reports, whether the system automatically assigns the person in charge of management. (5) In terms of records and reports, check whether the checklist contains the security issues of detection, information of the reporter, notes and annotation time, initial notes and annotation time of the reporter, credibility and confidentiality of the report, etc.

Assessment and decision stage (1) The level of personnel, including the testing qualifications of technicians and the qualifications for obtaining evidence, and whether the personnel performing emergency operations are on call around the clock. (2) In terms of records and reports, attention should be paid to the priority, completeness and confidentiality of the records, whether the records are guaranteed to have not been tampered with, and whether the forensic data is verifiable. (3) In terms of technology and processing methods, whether it has the same security event processing techniques and methods, whether it has provisions for handling security events that are occurring, whether technicians have compromised systems and all access to data, and whether they have access to external experts. (4) In terms of management system, whether there is a mature safety event classification system, a management system in which the response team and the evaluation team are connected, whether a safety and business risk assessment management process, a technical risk assessment process are established, and whether the employee and expert contact regulations and protection are established Suspicious data guide. (5) In terms of organization, we pay attention to the communication between different departments, including whether the technicians know how to contact the evaluation agency, external experts, detailed information providers, and other security response teams. In addition, in terms of notification release, the timeliness of internal notifications should be reviewed and whether relevant personnel have been notified to reduce activities.

Incident response stage (1) In terms of organization, whether the organization or personnel providing information to the third party should be established. (2) In terms of technology and processing methods, whether to ensure that unrelated personnel do not have access to information related to security incidents, whether technicians have control over the formulation, modification and execution of measures in the whole process of response, the control over the whole life cycle, whether the technician is responsible for the shutdown event after success, and whether the technician has the specific test on the adequacy, stability and functionality of safety events before incident response. (3) In terms of technical facilities, whether there are sufficient technical facilities to meet the requirements of evidence collection. (4) In terms of management system, the notification release system should review the timeliness of internal notifications and examine whether relevant personnel have been notified to reduce activities. In terms of process formulation, whether there are specific safety incident response regulations and regulations for monitoring the effectiveness of response. (5) In terms of records and reports, it should include targeted countermeasures and standard response lists, and whether confidentiality of forensic storage can be ensured.

Experience summary stage (1) In terms of management system, summarize methods and tools, and regularly assess their applicability and effectiveness, whether to set up a special incident response process applicability and effectiveness evaluation process, special incident response improvement process, special education difference review and training drills Process, specialized vulnerability management system, long-term security measures, whether to carry out safety event evaluation and latest information inspection, etc. (2) In terms of personnel level, the development department can or can't ensure that security vulnerabilities are adequately addressed. (3) In terms of technology and treatment methods, whether to ensure that similar or mutated security issues can be effectively addressed. (4) In terms of records and reports, whether the event cause report is fed back to the development department. Whether vulnerabilities, threats, and security incidents are updated in a timely manner in the public database. (5) Whether to form a complete safety incident handling report, summary report, and record of optimization improvement measures.

7.3 Review Method

According to the key elements of the review, the automotive cybersecurity incident response system can be simply determined by three ways of conformity, basic

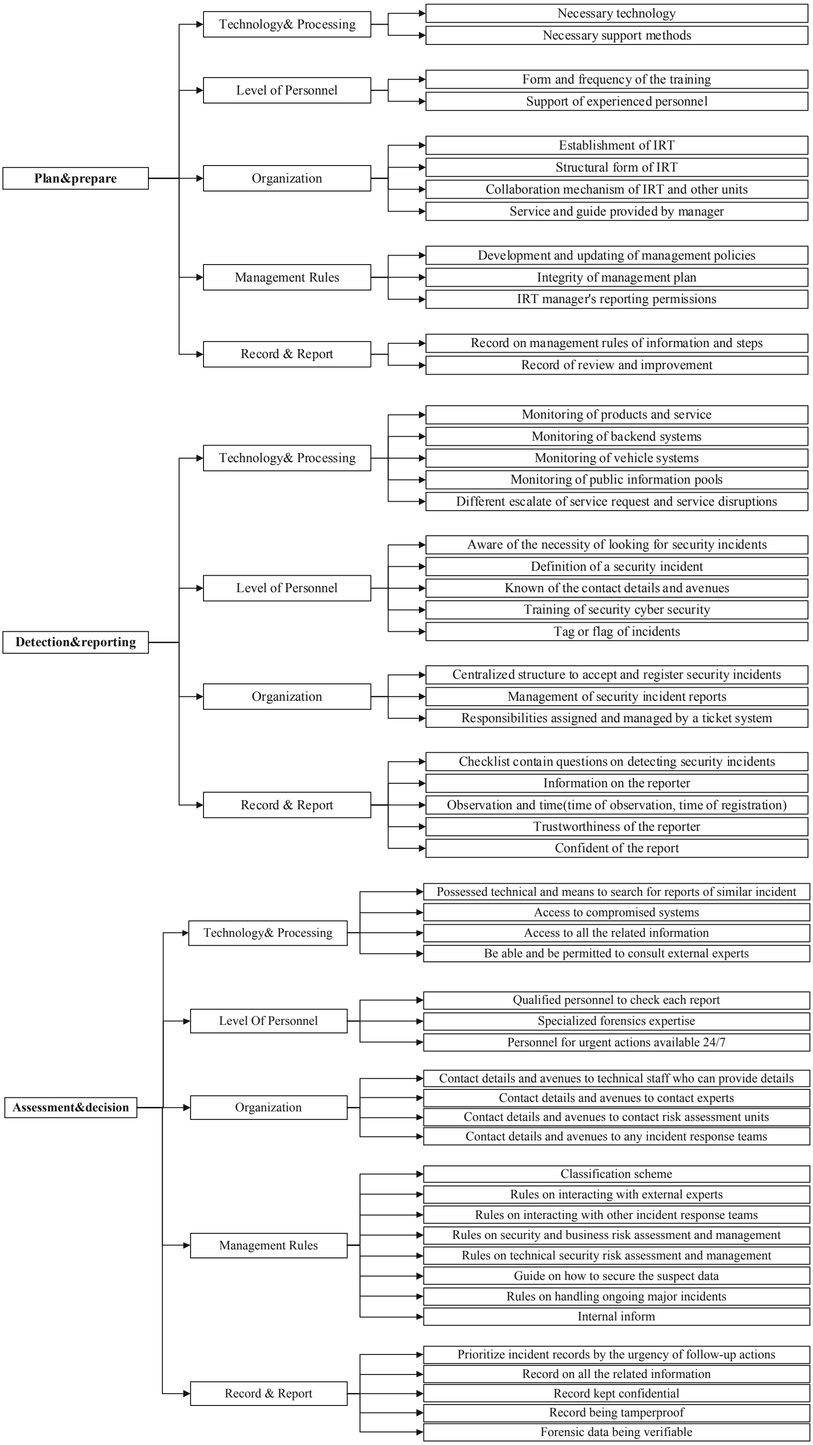
Plan&prepare
Technology& Processing
Necessary technology
Necessary support methods
Level of Personnel
Form and frequency of the training
Support of experienced personnel
Organization
Establishment of IRT
Structural form of IRT
Collaboration mechanism of IRT and other units
Service and guide provided by manager
Management Rules
Development and updating of management policies
Integrity of management plan
IRT manager's reporting permissions
Record & Report
Record on management rules of information and steps
Record of review and improvement
Detection&reporting
Technology& Processing
Monitoring of products and service
Monitoring of backend systems
Monitoring of vehicle systems
Monitoring of public information pools
Different escalate of service request and service disruptions
Level of Personnel
Aware of the necessity of looking for security incidents
Definition of a security incident
Known of the contact details and avenues
Training of security cyber security
Tag or flag of incidents
Organization
Centralized structure to accept and register security incidents
Management of security incident reports
Responsibilities assigned and managed by a ticket system
Record & Report
Checklist contain questions on detecting security incidents
Information on the reporter
Observation and time(time of observation, time of registration)
Trustworthiness of the reporter
Confident of the report
Assessment&decision
Technology& Processing
Possessed technical and means to search for reports of similar incident
Access to compromised systems
Access to all the related information
Be able and be permitted to consult external experts
Level Of Personnel
Qualified personnel to check each report
Specialized forensics expertise
Personnel for urgent actions available 24/7
Organization
Contact details and avenues to technical staff who can provide details
Contact details and avenues to contact experts
Contact details and avenues to contact risk assessment units
Contact details and avenues to any incident response teams
Management Rules
Classification scheme
Rules on interacting with external experts
Rules on interacting with other incident response teams
Rules on security and business risk assessment and management
Rules on technical security risk assessment and management
Guide on how to secure the suspect data
Rules on handling ongoing major incidents
Internal inform
Record & Report
Prioritize incident records by the urgency of follow-up actions
Record on all the related information
Record kept confidential
Record being tamperproof
Forensic data being verifiable

Fig. 1. Questionnaire framework for incident response system of automotive cybersecurity.

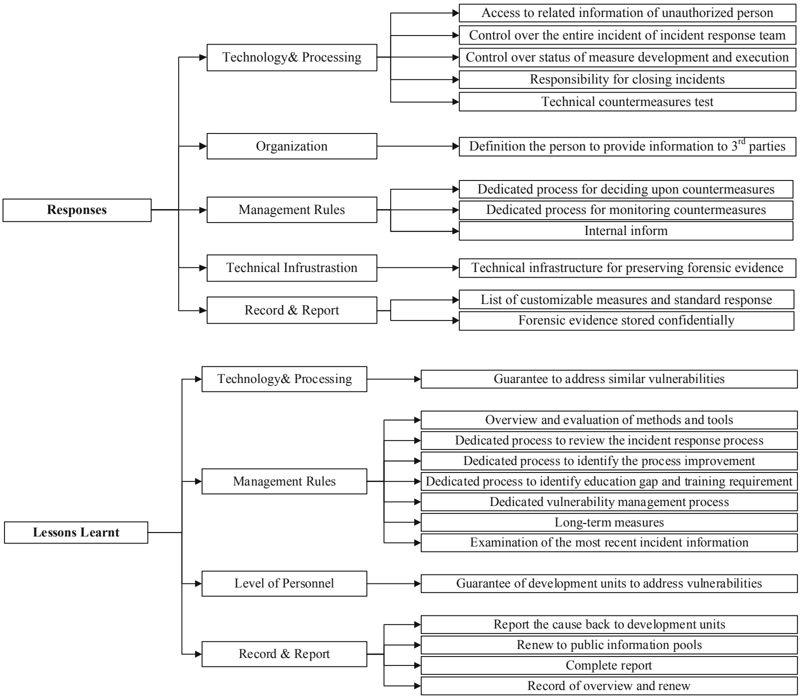
Responses
Technology& Processing
Access to related information of unauthorized person
Control over the entire incident of incident response team
Control over status of measure development and execution
Responsibility for closing incidents
Technical countermeasures test
Organization
Definition the person to provide information to 3rd parties
Management Rules
Dedicated process for deciding upon countermeasures
Dedicated process for monitoring countermeasures
Internal inform
Technical Infrustrastion
Technical infrastructure for preserving forensic evidence
Record & Report
List of customizable measures and standard response
Forensic evidence stored confidentially
Lessons Learnt
Technology& Processing
Guarantee to address similar vulnerabilities
Management Rules
Overview and evaluation of methods and tools
Dedicated process to review the incident response process
Dedicated process to identify the process improvement
Dedicated process to identify education gap and training requirement
Dedicated vulnerability management process
Long-term measures
Examination of the most recent incident information
Level of Personnel
Guarantee of development units to address vulnerabilities
Record & Report
Report the cause back to development units
Renew to public information pools
Complete report
Record of overview and renew

Fig. 1. (*continued*)

conformity and non-conformity. For the basic conformity and non-conformity of the project, should put forward guiding opinions or suggestions.

According to the questionnaire, the incident response system is reviewed from the aspects of conformity, applicability, pertinence, completeness, scientific, formativeness and cohesiveness. For detailed review, the review elements can be reviewed separately by means of a list. When reviewing the emergency plan, the elements of the emergency plan are analyzed correspondingly with the review contents and requirements in the table to determine whether the requirements in the table are met, and problems and deficiencies are found (Fig. 1).

8 Summary

In this paper, the construction method of automobile cybersecurity incident response system is given, and a questionnaire is designed to evaluate the incident response system. The system is suitable for OEMs, parts supplier, third party organization, etc. In addition, the complexity and cross-regional nature of the Internet determine that the incident response of cybersecurity incidents should be a collaborative process of multiple departments and units, which requires the competent departments and emergency agencies to constantly integrate their respective advantages, and ultimately form a joint effort to cope with the problem of automobile cybersecurity.

At present, automobile cybersecurity presents the characteristics of attack organization, profit-making, innovation of attack methods, instrumentalization and platform of attack technology. At the same time, it also faces many problems and challenges: complex and changeable environment at home and abroad, lack of core technology and equipment, and relatively backward cybersecurity guarantee work. In this regard, the following suggestions are given:

(1) Adhere to the incident policy of quick control in emergencies and service focus in normal times;
(2) Carry out systematic confrontation in incident treatment;
(3) Clarify the responsibilities and obligations of cybersecurity hazards;
(4) Complete the cybersecurity organization system and strengthen the emergency rescue system;
(5) Implement the administrative execution ability and enforcement power of the incident response subject in the mechanism;
(6) Change the incident response after the event to the incident response before and during the event;
(7) Conduct regular national-level cyber security emergency drills.

References

1. Creasey, J.: Cyber Security Incident Response Guide. CREST, Bengaluru (2013)
2. Choucri, N., Madnick, S., Koepke, P.: Institutions for cyber security: international responses and data sharing initiatives. In: Working Paper CISL (2016)
3. Shen, X.: Research on Network Security Emergency Response Linkage System. Hubei University of Technology, Wuhan (2009)
4. De Muynck, J., Portesi, S.: Strategies for Incident Response and Cyber Crisis Cooperation. ENISA, Heraklion (2016)
5. ISO/IEC 27035-1: Information Technology-Security Techniques - Information Security incident management-Part 1: Principles of Incident Management (2016)
6. ISO/IEC 27035-2: Information Technology-Security Techniques - Information Security Incident Management-Part 2: Guidelines to Plan and Prepare for Incident Response (2016)
7. Liu, X., Li, B., Chang, A., Hui, L., Tian, Z.: The current network security situation and emergency network response. Strateg. Study Chin. Acad. Eng. **18**(6), 83–88 (2016)
8. GB/T 28448-2012: Information Security Technology-Testing and Evaluation Requirement for Classified Protection of Information System (2012)
9. Loukas, G., Gan, D., Vuong, T.: A review of cyber threats and defense approaches in emergency management. Future Internet **5**, 205–236 (2013)
10. Ma, H.: The Research of Network Security Emergency Response System Based on CBR. Shanghai Jiaotong University, Shanghai (2010)
11. Rico, S., et al.: Incident Management and Response. ISACA, Rolling Meadows (2012)
12. GB/Z 20986-2007: Information Security Technology-Guidelines for the Category and Classification of Cybersecurity Incidents (2007)
13. Chunfei, W.: Database Design of the Cybersecurity Vulnerability Database and Implementation of the Management Platform. Beijing University of Posts and Telecommunications, Beijing (2011)

14. Zhang, Y., Lu, S., Qiu, L.: Research and practice of information security emergency handling mechanism based on event. Information Security and technology (2015)
15. Practice Guide for Information Security Incident handling. Hong Kong: Office of the Government Chief Information Officer (2017)
16. Loukas, G., Gan, D., Vuong, T.: A review of cyber threats and defense approaches in emergency management. Future Internet **5**(2), 205–236 (2013)
17. Kämppi, P., Rathod, P., Hämäläinen, T.: Cybersecurity safeguards for the automotive incident response vehicles. In: Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, pp. 291–298. SCITEPRESS-Science and Technology Publications, Funchal, Madeira (2017)
18. Hao, Y.: Research on Risk Quantification Method of Cybersecurity. Dalian University of Technology, Dalian (2016)