Automotive Cyber Maturity Report 2025

Dr. Teresina Herb, Michael Klinger,
Dr. Robert Lambert, Dr. Moritz Minzlaff

Empowering Tomorrow's Automotive Software
www.etas.com

Contents

Preface

Rapid changes, such as those occurring in the automotive industry, require quick adaptation by market participants to stay competitive. Quickly adapting to changing environments, however, has long been a core capability for mastering cybersecurity in the face of a continuously evolving threat landscape. And so, the question of increasing an organization's cyber maturity and moving ahead of the competition are inexorably linked.

Vehicles and their components are undergoing three major technological transformations: the move to centralized E/E architectures, the decoupling of software and hardware, and the integration of artificial intelligence. So it comes as no surprise that cyber maturity is a concept that must be understood on both an organizational and a technological level. Security is one key dimension to ensuring and maintaining vehicle health over its lifetime.

But cybersecurity comes with its own challenges. Markets move at different speeds in adopting new regulatory requirements or new technology. Artificial intelligence is a technology moving from hype to product, necessitating solutions for its secure and complaint use. At the same time, cyber incidents have become commonplace, requiring automotive companies to both embrace new technologies and secure them simultaneously.

Forward thinking, highly cyber-mature organizations see security as contributing to a larger push to advance management of vehicle systems, which leads to higher efficiency and reduced costs while meeting security requirements and expectations. I thank everyone who participated in our survey and wish you, dear reader, many useful insights from reading this year's Automotive Cyber Maturity Report.

"Security is one key dimension to ensuring and maintaining vehicle health over the lifetime."

Mariella Minutolo
Executive Vice President Sales

Executive summary

Insight #1: Organizational and technical cyber maturity are in lockstep

Companies with high cyber maturity remain characterized by end-to-end consideration of security over three dimensions: product lifetimes, ecosystems, and software supply chains. They promote DevSecOps practices for security over product lifetimes, and are concerned with ecosystem components such as backends, but also software supply chains and bills of material. They employ multi-framework cybersecurity management systems that reflect standards from multiple markets, and they are aware of and prepared for incidents. At high-maturity organizations, organizational and technical cybersecurity are synergistic and move forward in lockstep.

Insight #2: As GenAI moves from hype to product, security automation gains ground

Generative AI (GenAI) transforms automotive security by enhancing threat detection, vulnerability discovery, secure software development and innovation/competitiveness, but also elevates risk when wielded adversarially by attackers. Nevertheless, the level of hype for GenAI has subsided, particularly in China. Overreliance on AI decision making is seen to have the potential of decreasing situational awareness. Most participants report moderate or high levels of DevSecOps deployment, with Europe and US slightly ahead, while China is rapidly catching up.

There is a growing demand for security tooling, but the heterogeneity of tools is seen as a major challenge. Generally, there is little preference between in-house and vendor-supplied tools, though qualified experts prefer in-house. Regionally, Japan has fewer in-house developments. Semiconductor suppliers prefer in-house tooling. Upper management prefers tools from vendors, integrated by third parties.

Insight #3: Cyber incidents have become commonplace

Incidents have become prevalent: 60% of our participants are aware of a security incident and 20% of a safety incident (rising to 40% in China). Increased incident awareness correlates with maturity, time spent on cybersecurity, higher managerial level and cybersecurity expertise.

Threat intelligence comes from many sources, but easer-to-access sources are more popular, especially in low-maturity organizations, whereas the deep and dark web become more popular among high-maturity organizations and qualified experts. Higher maturity organizations involve more internal departments in the resolution of incidents, and are more likely to have dedicated departments for this purpose.

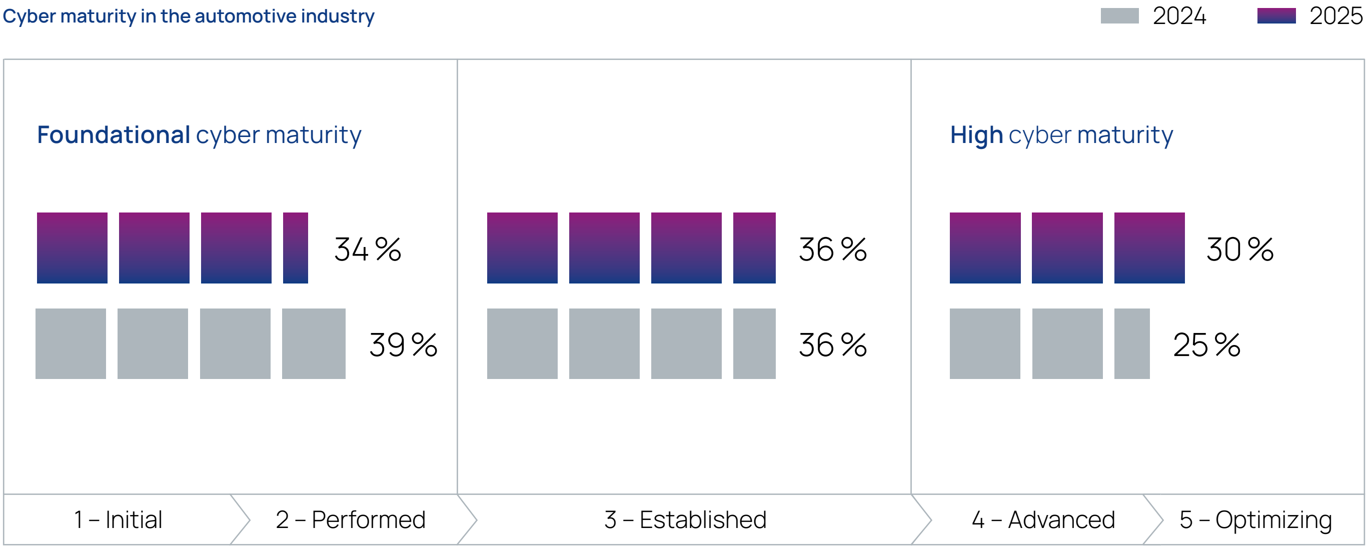
Insight #4: Regional security regulations in times of global politics

This year, regional regulations have gained importance in line with geopolitical trends. However, as in previous years, regulatory compliance remains the primary motivation for cybersecurity – especially among less mature organizations. Cybersecurity responsibility is shifting from R&D to Information and Product Security departments.

The top four security frameworks have not changed since 2023: ISO/SAE 21434, UNECE R155, ISO 26262 and UNECE R156, but China's regulations have also increased in importance in Europe and locally. Chinese participants also rate EU regulations as very important. Among US participants, US frameworks are considered most important (52%), followed by European ones (45%), while Chinese frameworks rank lower overall (23%) – though this rises to 70% among Chinese participants.

Generally, organizations focus first on regulations in their local market, then on international and European standards – except in Europe, where the secondary focus is on China.

Cyber maturity in the automotive industry



Context and design of this year's survey

With its 5th edition, the ETAS Cyber Maturity Survey has now definitively established its place and importance in the automotive cybersecurity community.

The survey targeted automotive professionals whose work involves various aspects of security — ranging from security engineers and production specialists to C-level executives — offering a comprehensive view of how organizations in the automotive sector address security challenges and assess their own performance in this important field.

New topics in 2025 are:

1. sourcing security solutions and participants' preferences wrt. integration of solutions in-house vs. third parties,
2. most concerning type of cyber incident in area of responsibility and organizational units involved in resolution and
3. in-vehicle security measures implemented in company products.

Starting this year, we have introduced insights on cyber maturity topics provided by qualified experts. From the total of 174 participants, approximately 10% are part of the expert group (see below).

The survey includes 25 questions (19 + 6 background information), it was conducted anonymously over the course of one month, participants provided their responses on multiple-choice and quantitative assessment questions.

Qualified experts and general automotive professionals

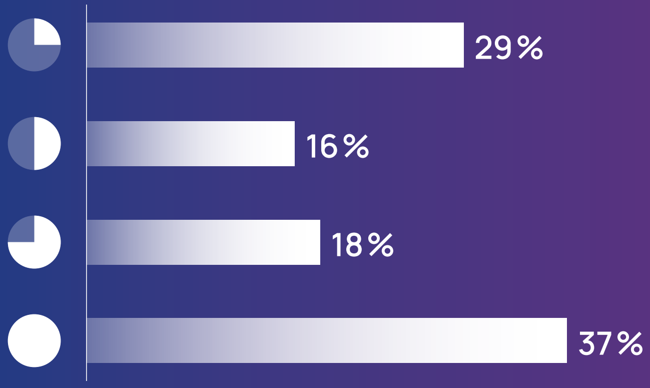
This year we added "qualified experts" as a control group to our survey. While the survey participants have always included security experts, the survey's anonymity prevented us from identifying them as a group and drawing comparisons between their answer behavior and that of general automotive professionals. For the 2025 survey, Auto-ISAC members selected one participant each from their respective companies who met the following criteria to be a qualified expert:

- at least five years in automotive security,
- current role has a security focus, and
- has a good grasp of the company's cyber maturity beyond their immediate area of responsibility.

The individuals remained anonymous to us, but participated through a special link that allowed identification as a qualified expert. We thank Auto-ISAC and its membership for this very productive cooperation in strengthening cybersecurity insights.

Survey statistics

Time dedicated by participants to cybersecurity-related tasks

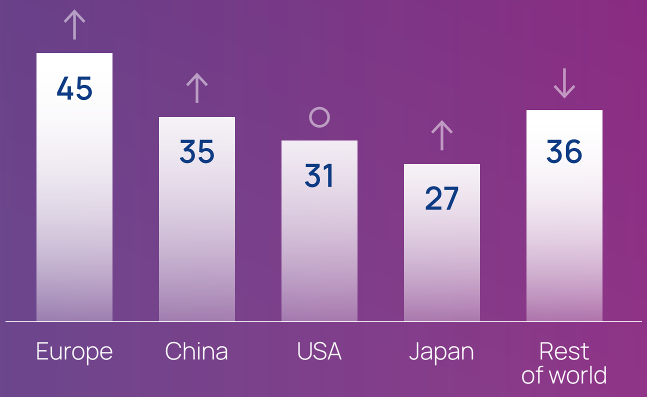


Regional participation

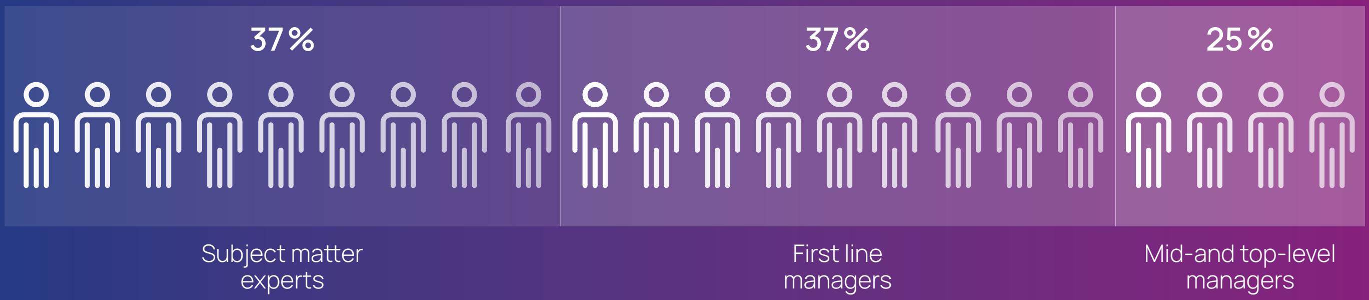
↑ increase or

↓ decrease compared to previous year

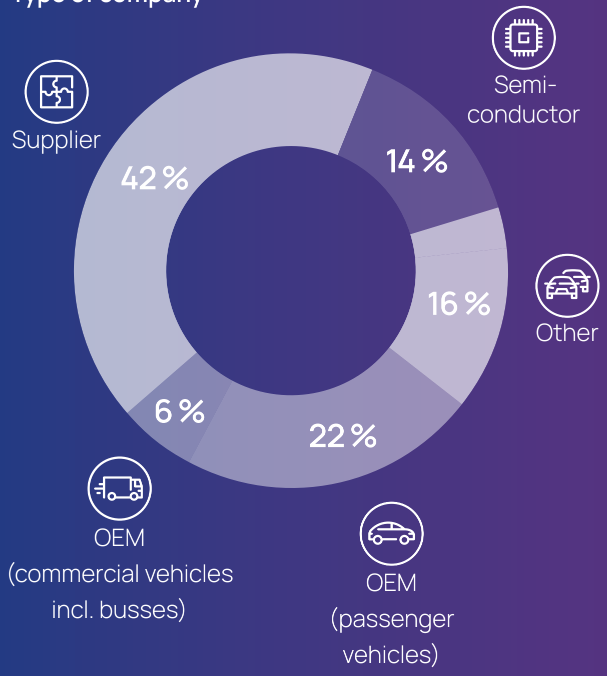
Total number of participants: 174



Job level of participants

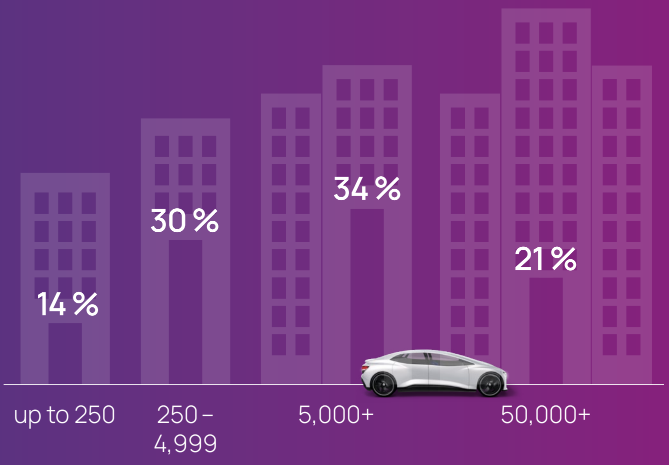


Type of company



Size of company

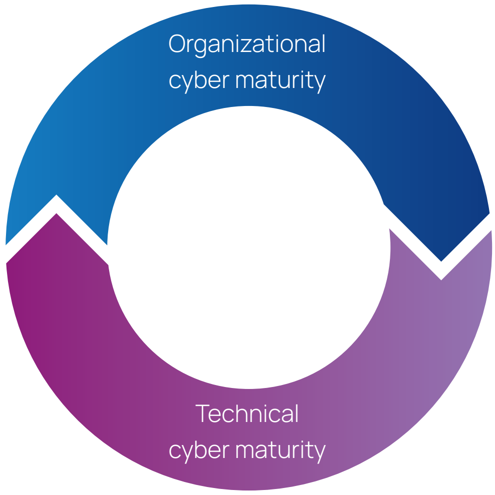
measured in number of employees



Key insights

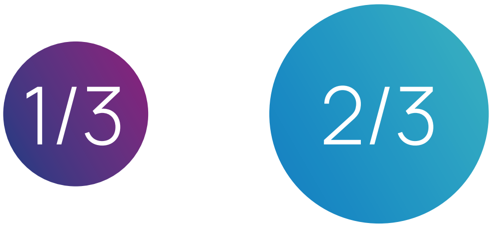
Insight #1: Organizational and technical cyber maturity are in lockstep

In our 2023 report, we stated that high cyber maturity is characterized by end-to-end thinking in three dimensions: the product's lifetime, its ecosystem, and its software supply chain. This is still true: Participants from highly mature organizations demonstrate a significantly greater tendency to consider the broader ecosystem in the attack surface such as vehicle backends (+18%pts over foundational maturity) or mobile devices (+15%pts). They also report a considerably higher adoption of DevSecOps practices that are crucial to maintain adequate security over product lifetimes.



Additionally, this year's results show that organizational cyber maturity and technical cybersecurity are closely linked concepts. For a company to advance in cyber maturity, it must do so on both levels, as organizational measures are most effective when supported by technical capabilities in the product, and vice versa. In fact, adoption rates of in-vehicle measures are among the clearest separators of high and foundational cyber maturity in the 2025 survey: Eight of the nine measures are implemented by the majority of high-maturity organizations, the only exception is UDS 29, which still comes in at 44%. In contrast, at foundational cyber maturity only HSM and secure boot are implemented by more than half. The average adoption rate of in-vehicle measures is 65% versus 36%. The data paints a similar picture for offboard measures. Organizational cyber maturity and technical cyber maturity are in lockstep.

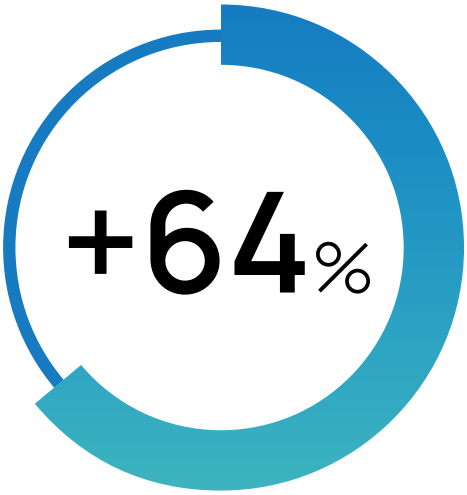
Average implementation rate of in-vehicle security measures:



among foundational maturity organizations

among high-maturity organizations

Other areas that distinguish high-maturity companies are cyber incidents and multi-framework cybersecurity management systems (CSMS). Cyber maturity correlates with incident awareness (+18%pts), higher adoption and broader scope of threat intelligence, as well as better preparedness for upcoming incidents. We discuss cyber incidents in greater detail in the third insight.



More frameworks considered by **high maturity**

Multi-framework CSMSs tackle regulatory cybersecurity requirements from different markets while addressing numerous industry and government standards; which is another feature of high cyber maturity. These management systems go beyond an ISO/SAE 21434 or UN R 155 baseline and integrate obligations - for example, from the China GB and GB/T series. Note that the Chinese standards also include technical requirements, potentially highlighting a different approach to regulation, but also underlining that organizational and technical cybersecurity go hand in hand. You will find more on the topic of frameworks in the fourth insight.

However, the type of company does not make a significant difference influencing average cyber maturity. Across different segments, the results show similar ranges for high-maturity organizations – only the semiconductor sector appears to be more advanced. Conversely, similar percentages of participants selected foundational and mid-maturity levels for their organization, regardless if from an automotive manufacturer, a supplier, or a semiconductor company. A notable exception are responses from commercial vehicle manufacturers: No one selected mid-level maturity. They consider themselves either at the beginning or the high stages of cyber maturity.

Insight #2: As GenAI moves from hype to product, security automation gains ground

Generative AI is transforming automotive security by enhancing threat detection, vulnerability discovery, and secure software development. It enables real-time analysis of vehicle data, simulates cyberattacks, and supports digital twin testing environments. GenAI also improves code security and allows intuitive natural language interfaces for monitoring. However, it introduces risks such as adversarial use by attackers, model exploitation, and data privacy concerns. Overreliance on AI decisions can also be problematic. As vehicle manufacturers adopt AI-driven cybersecurity tools, regulatory standards like ISO/SAE 21434 are evolving to address these changes. GenAI offers powerful tools, but careful implementation is essential for safety and trust.

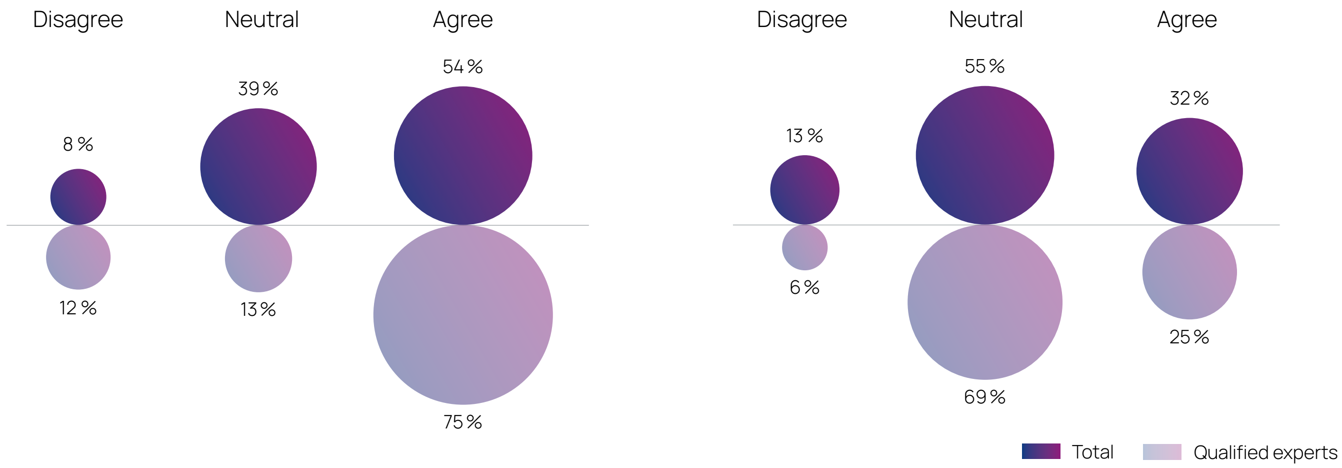
The general trends and perception in automotive security are confirmed by the results of this year's Cyber Maturity Survey: Most respondents believe AI increases competitiveness and is crucial for cybersecurity innovations.

The group of qualified experts have a more positive view on the introduction of GenAI when compared to the remaining participants. In particular, they view its impact on automotive security as crucial for innovation and enhanced competitiveness. In contrast, the qualified experts have a rather neutral position with regard to introduction of additional vulnerabilities through GenAI.

How would you assess the influence of Generative AI (GenAI) on automotive security?
Rate your level of agreement with the following statements:

GenAI is crucial for future innovations in automotive cybersecurity.

GenAI introduces more vulnerabilities than solutions in automotive cybersecurity.

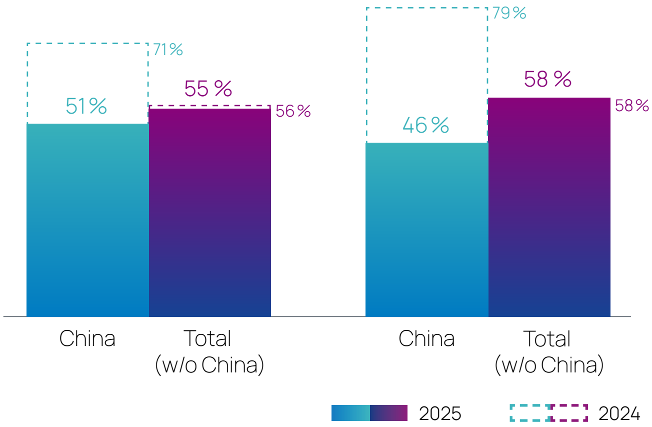


Additionally, we observe that generally the hype on GenAI has slowed down. The participants' views center around neutral responses for both vulnerabilities and innovation/competitiveness questions. Responses at the extremes (strongly agree/disagree) dropped significantly compared to the previous year.
Compared to 2024, the responses from China and Japan more closely align with those from Europe and North America; consequently, perceptions across these regions show minimal differences. However, the hype disillusion is very prevalent in Chinese figures, with a drop for innovation and competitiveness of ~20% from 2024 to 2025.

Additional confirmation can be derived from the responses on technical security solutions: The answer option for GenAI received a comparable number of votes in 2024 and 2025, and did not change its position in the overall field of responses. A similar pattern exists for cybersecurity challenges, here GenAI maintained a stable position in the upper center field.

GenAI is crucial for innovations in cybersecurity

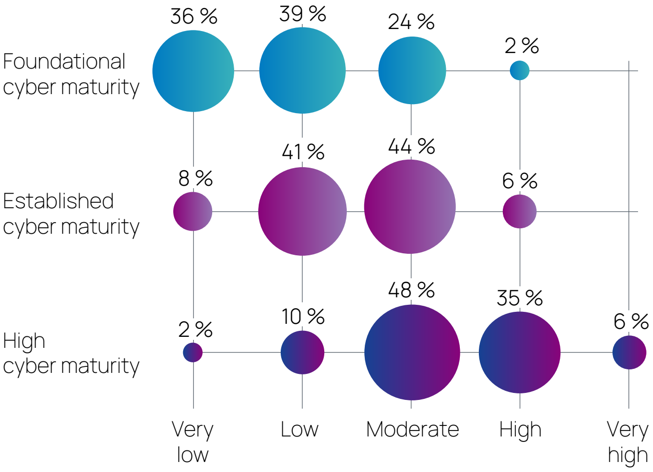
Beyond cybersecurity, GenAI enhances the competitiveness



Looking into the different company backgrounds of the survey participants, we deduce that commercial vehicle manufacturers seem to be slightly more skeptical with regards to the threats introduced by GenAI. However, the position on innovation and competitiveness is rather homogeneous throughout the industry. The company size has limited impact on the voting results; participants from small enterprises tend to have rather neutral views in competitiveness and innovation compared to others.

Automation tools enhance development and security by streamlining workflows, reducing errors, and improving efficiency. In development, tools like CI/CD pipelines, linters, and infrastructure-as-code solutions accelerate code integration, testing, and deployment. In security, automated scanners, dependency checkers, and secrets detection tools help identify vulnerabilities early and enforce compliance. These tools enable faster delivery, consistent standards, and scalable operations while strengthening security. DevSecOps teams can collaborate more effectively, respond to threats proactively, and maintain high-quality, secure software throughout the development lifecycle. The majority of the survey participants consider themselves at least moderate with regard to implementation of DevSecOps practices (38%) and 15% consider themselves to have a high or very high adoption. In the survey results we see a correlation with maturity level (high maturity correlates with high adoption of DevSecOps) with minor regional differences: Europe and US are slightly stronger, while China is catching up. Closely linked to the implementation of DevSecOps is the integration and use of tools (see next chapter).

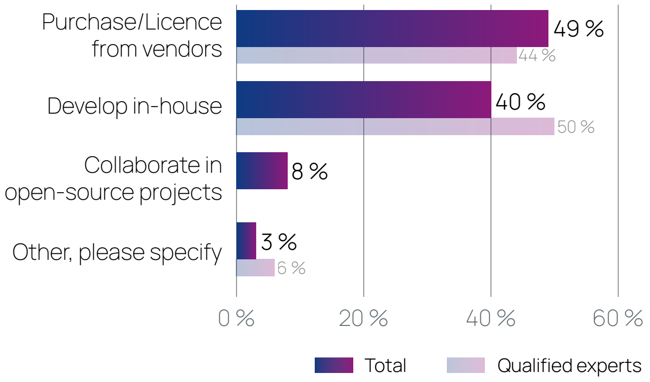
How do you rate your company's current level of adoption of DevSecOps practices?



OEMs and suppliers adopt the trends of IT business and increase automation in their approaches and processes. This also applies to security aspects – hence driving a demand for the respective tooling. However, from the Cyber Maturity Survey responses, we see that about 42% of respondents consider capabilities and heterogeneity of tools a challenge.

We learn that survey participants equally intend to purchase solutions from vendors (incl. license) or develop them in-house. We see some especially strong opinions for in-house implementations, which are not seen for third-party integration. Diving further into the details reveals that the general respondent seems to have no specific preference, as there is an almost equal distribution for neutral, in-house and third-party responses, however qualified experts have a clear preference for in-house integration.

In your area of responsibility, what approach do you prefer for sourcing security solutions?



There are some interesting regional differences: For Japan, there is less in-house development, but more collaborative open-source projects. The same is reflected in their general preference for in-house integration.

Semiconductor suppliers have a strong preference for in-house developments, while all other have tendencies towards purchasing from vendors. A similar picture forms when looking into integration preferences.

The survey responses show a clear preference to source from vendors at mid/top management, and a slightly stronger preference to have third-party integration at mid/top management.

Insight #3: Cyber incidents have become commonplace

Incidents have become commonplace. Our respondents were made aware of security and safety incidents in their products at a surprisingly high rate:

– 60% aware of a security incident,

– 20% aware of a safety incident, and

– 40% in China aware of a safety incident.

China is also the region where lessons learned from incidents are the main drivers for cybersecurity.

Increased awareness of incidents is correlated with organizational maturity, the amount of time an organization spends on cybersecurity, and the respondent's managerial level. Our qualified experts also spend more time on cybersecurity; accordingly, three-quarters of them are aware of incidents, compared to less than half of general professionals.

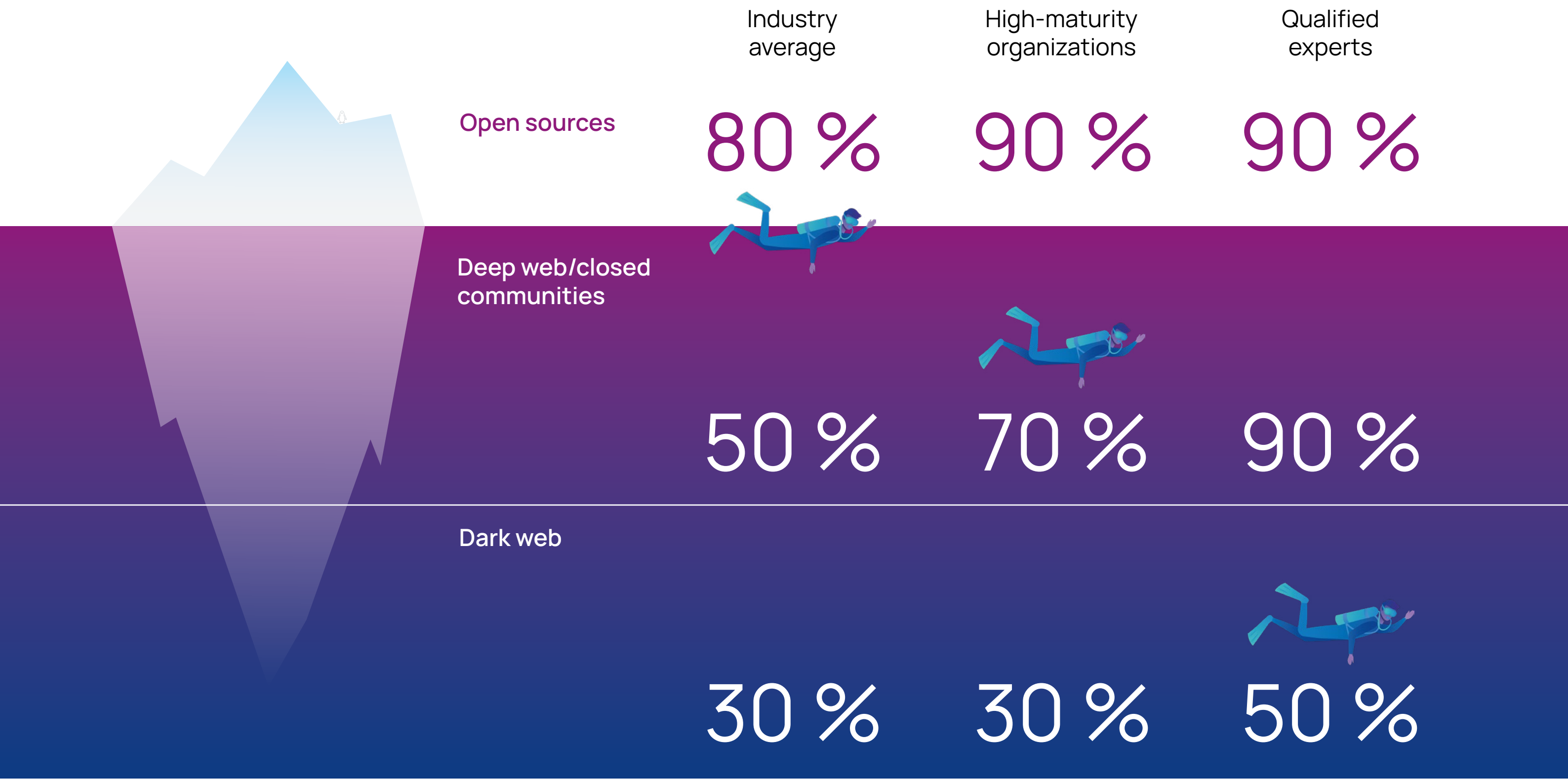
Beyond spending more time and possessing greater security expertise, having a higher managerial level may also allow for visibility into more incidents and increasing overall awareness.

A concerning inference might be made that organizations which perceive fewer incidents may actually just be unaware of threats that exist in reality.

Multiple classes of cyber threat intelligence are used by our respondents. The more difficult it is to access a source, generally, the less likely it is used for threat intelligence: Open sources score highest, followed by closed communities and then lastly the deep web and the dark web.

Both high-maturity organizations and our qualified experts dive deeper into threat intelligence, looking beyond open sources to the deep web and closed community sources and also to the dark web.

What types of sources for cyber threat intelligence do you consider in your area of responsibility?



When incidents are to be resolved, higher-maturity organizations are more likely to involve more other departments and functions in the incident resolution. This may stem from the development of specialized incident response organizations in these organizations.

Managerial level also is correlated with involving more functional groups in incident resolution.

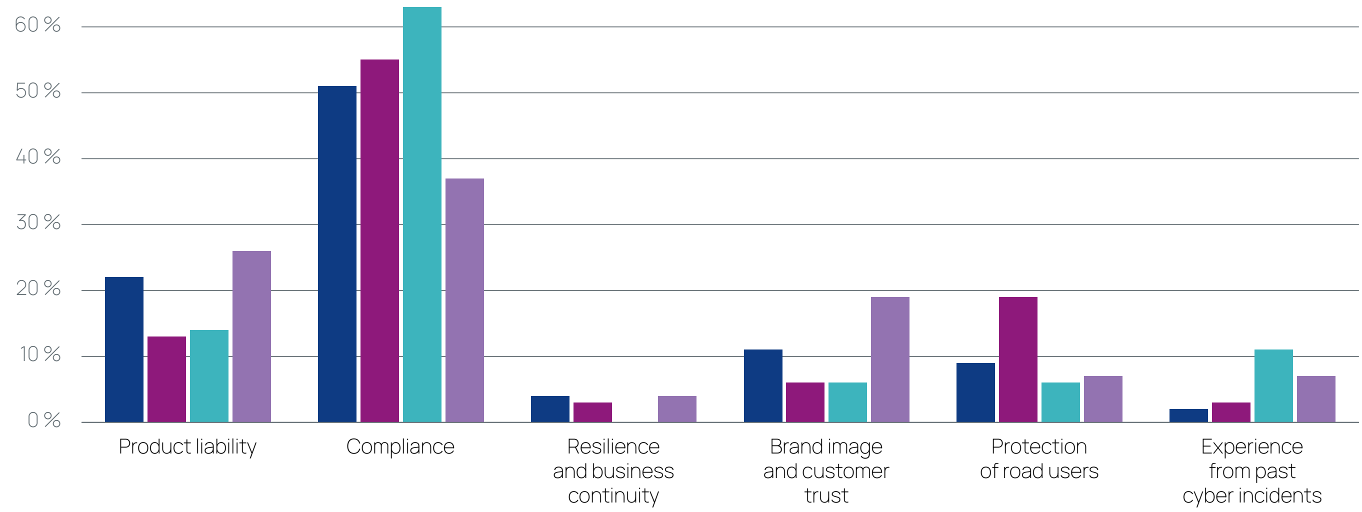
The top four teams likely to be involved in incident resolution are Communications, Governance/Compliance, Manufacturing, and Legal. In high-maturity organizations, R&D, Security, and IT departments are also likely to be involved.

Insight #4: Regional security regulations in times of global politics

This year, we observe the growing importance of regional regulations, their increasing impact on business strategy and correlation with the geopolitical trends.

As in previous years, the main driver to implement cybersecurity is compliance to regulations and standards, with a similar distribution in all regions. We can observe that this compliance has a higher importance in organizations at the lowest maturity level.

What is the primary driver for cybersecurity in your area of responsibility?

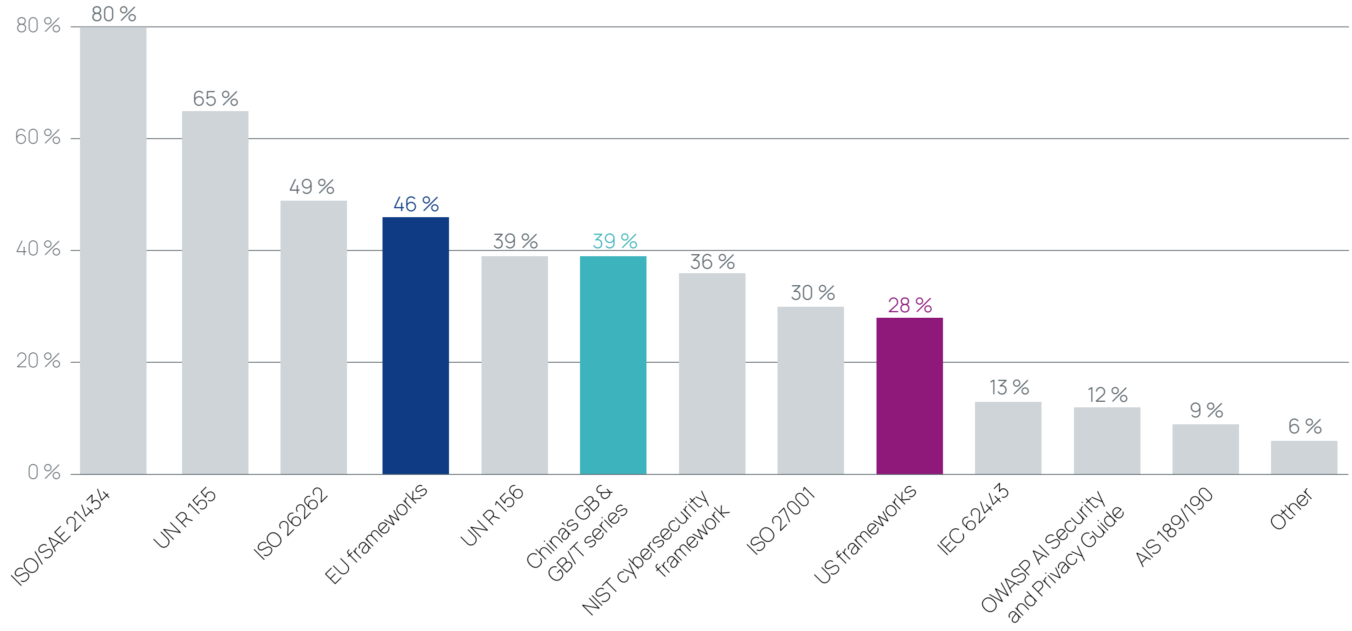


Even if the Research and Development department is still the main area responsible for product security, followed by the Product Engineering department, we can observe an important responsibility shift to the Information/Product security department, without any difference between regions.

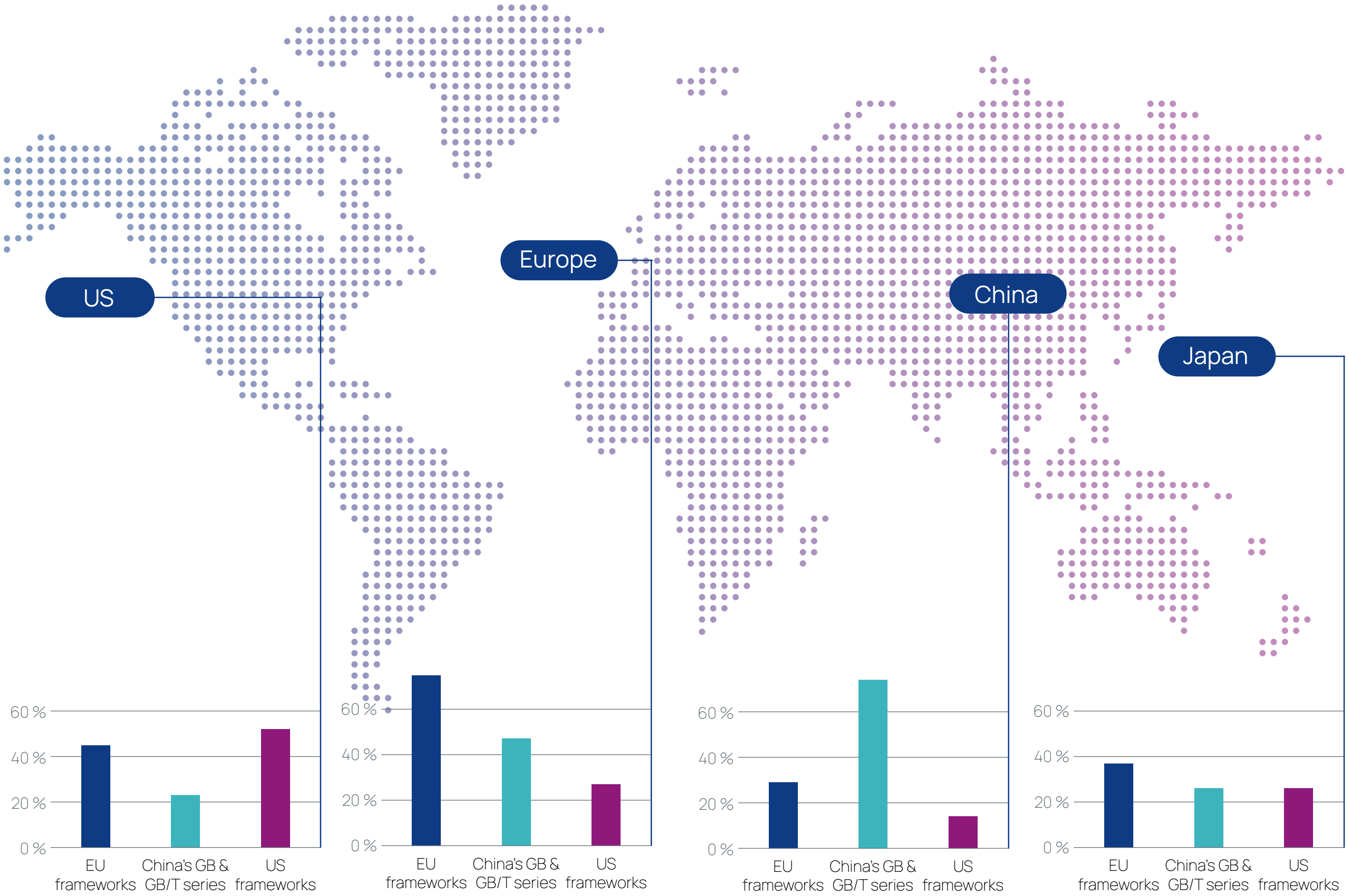
Regarding the frameworks considered, the top 4 have not changed since 2023: ISO/SAE 21434, UNECE R155, ISO 26262 and UNECE R156.

Mirroring our approach for China's GB & GBT series (which regroups Chinese regulations and standards), if we aggregate European regulations (EU Cyber Resilience Act, VDA ASPICE for cybersecurity, EU NIS 2 Directive) and US regulations (NHTSA Cybersecurity best practices, US DoC's Securing… Supply Chain), this leads to the following distribution:

Which frameworks do you consider for cybersecurity in your area of responsibility?



We can also observe that regional frameworks have become very important.
Let's now take a look at the distribution of these frameworks based on the participants' regional origin:



As expected, European participants focus on ISO/SAE 21434 and UN R 155, in addition to the EU frameworks. With 44%, Chinese frameworks also have a strong focus.
This aligns with expectations, considering most of the European automotive players communicate their interest in the Chinese market.

For US participants, the leading three cybersecurity frameworks are ISO/SAE 21434, UN R 155 and NIST. Focusing on regional frameworks, US frameworks are primarily important (52%), followed by the European ones (45%). It is interesting to observe that the Chinese frameworks are only at 23%. These numbers corelate to the geopolitical situation.

We can observe that Chinese participants are mainly concerned with Chinese frameworks (more than 70%) followed by ISO/SAE 21434. The international frameworks are also taken into account (from almost 60% for the UN R 155 to 20% for the ISO 27001). The numbers also confirm Chinese interest in the European market, as the EU frameworks are at the same level as the UN R 156 with 29%, but interest in US framework is lower (at 14%).

Finally, Japanese participants focus on ISO/SAE 21434, UN R 155 and ISO 26262, followed by the EU frameworks and the UN R 156 (37%). Chinese and US frameworks are at the same level with 26%.

For the other regions, we can observe the same main focus on international standards, followed by the EU frameworks (33%), US ones (22%) and China (17%).

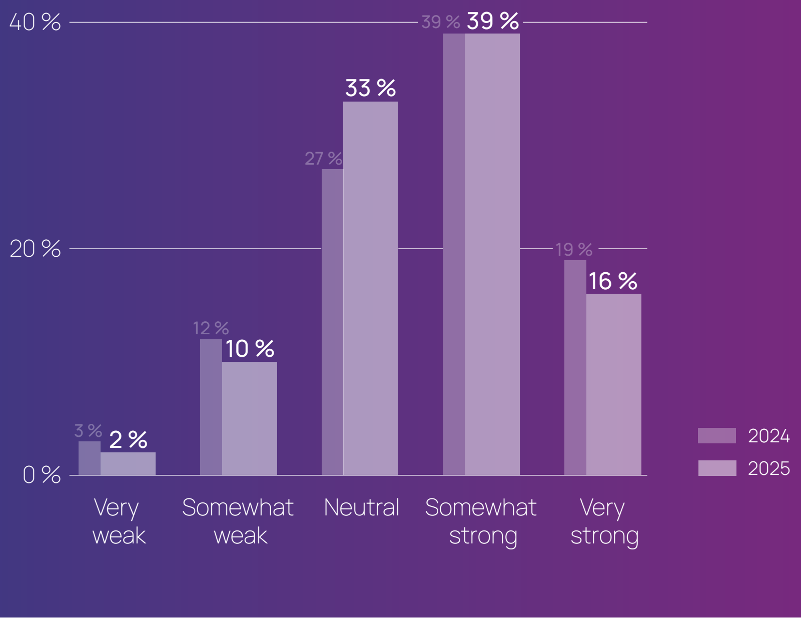
As expected, high-maturity companies take into account all frameworks and regulations, but less mature companies are regionally focussed. Qualified experts and mature companies answered in similar ways.

With these graphics, we can perceive that organizations focus first on their local market, and then on Europe (except in Europe, which has a secondary focus on China).

Survey results in detail

1. How would you rate your company's position in the market in comparison with its competitors? (single answer)

When rating their company's competitive position, Europe and the US are the most confident, while China and, in particular, Japan are more neutral. Compared to the previous year (2024) especially in Europe and US we see a strong trend towards positive rating of own market position. China and Japan remain stable neutral. All regions have a clear trend to positive self-perception compared with 2024.

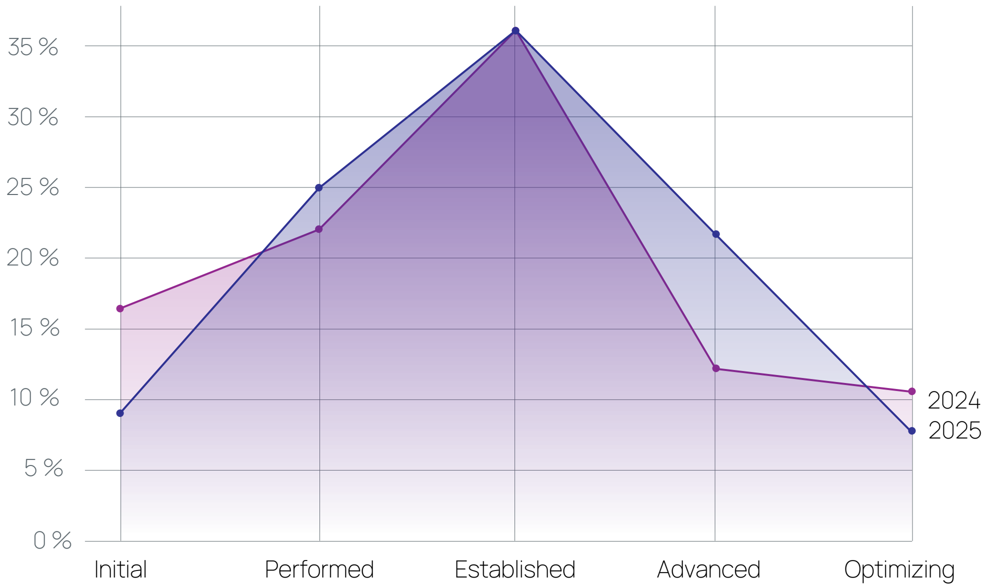


2. Overall, how would you rate the cyber maturity of your company?

(single answer)

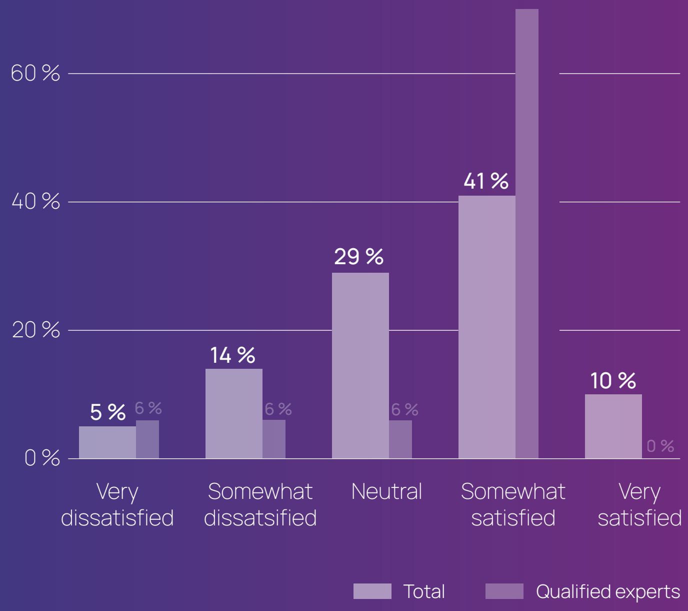
Fewer participants than ever rate their company at the initial maturity level. However, overall the industry is roughly split into three groups: one third at levels 1 and 2, one third at level 3, and one third at levels 4 and 5.

Among the regions, European participants consider their companies significantly more mature than those from other regions, showing the strongest skew toward the highest maturity levels, while participants from the US and China tend to cluster more around the middle levels.



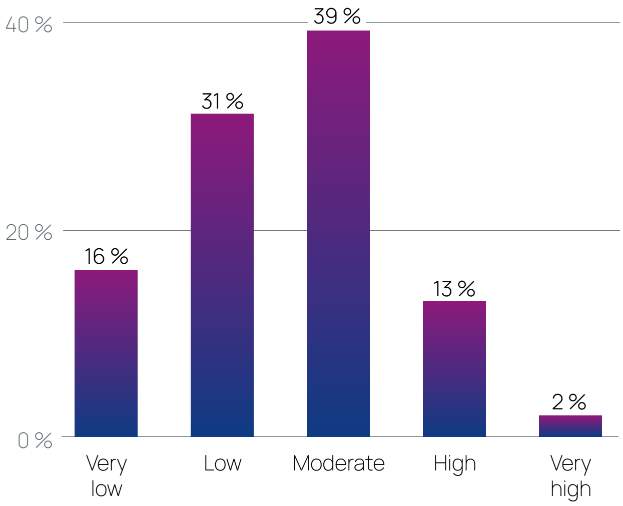
3. How satisfied are you with the progress regarding cybersecurity in your area of responsibility since last year? (single answer)

Overall satisfaction in the industry indicates small but steady progress, with an outlook, on average, that is slightly positive and similar to last year. Qualified experts with their more comprehensive view are considerably more satisfied with the progress than general professionals.



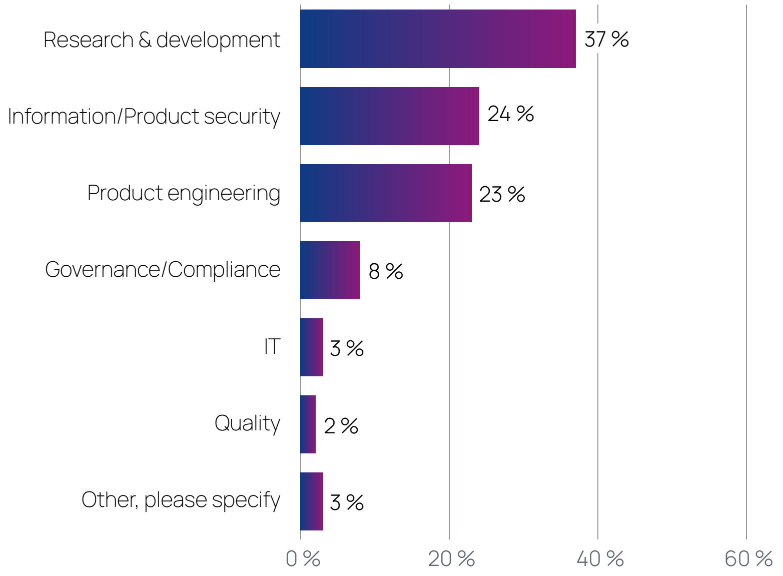
4. How do you rate your company's current level of adoption of DevSecOps practices? (single answer)

The data shows a strong correlation between cyber maturity and adoption of DevSecOps practices. The responses show that the industry is still in the early phases of implementing DevSecOps with 85% of participants reporting at most a moderate adoption.



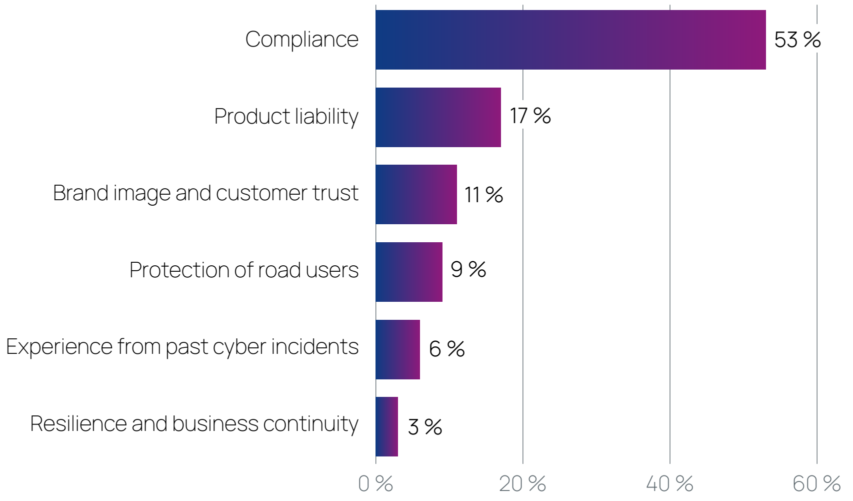
5. Which organizational unit is primarily responsible for product security within your company? (single answer)

With an increase of cyber maturity, the responsibility shifts from R&D and product engineering to dedicated information/product security roles. Together with compliance/governance, these dedicated roles are the leading units for product security at the majority of high-maturity companies.



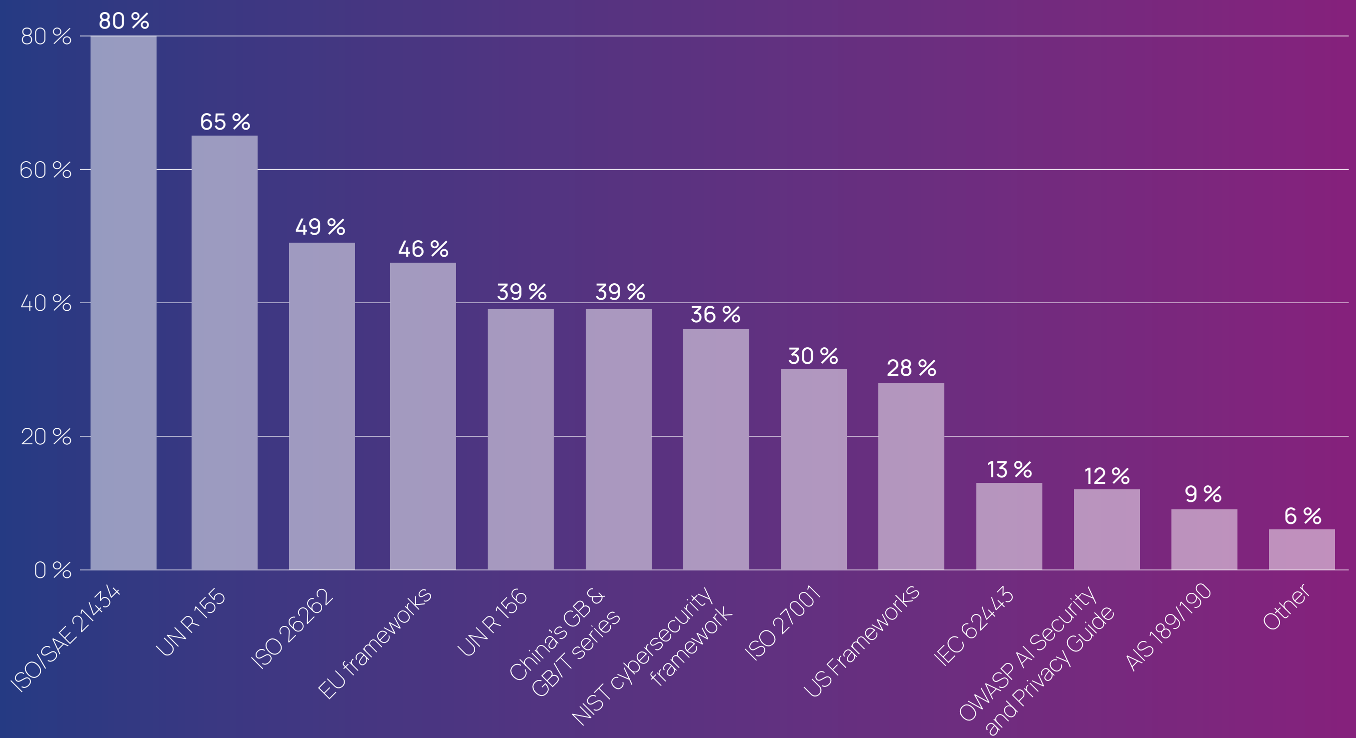
6. What is the primary driver for cybersecurity in your area of responsibility? (single answer)

The main driver for cybersecurity amongst survey participants is compliance. While this holds across all segments, higher maturity companies are motivated more often by other aspects as well. Experience from past incidents comes in second to last but is in the top 3 for participants from China, as well as those from companies with few employees.



7. Which frameworks do you consider for cybersecurity in your area of responsibility? (multiple answers)

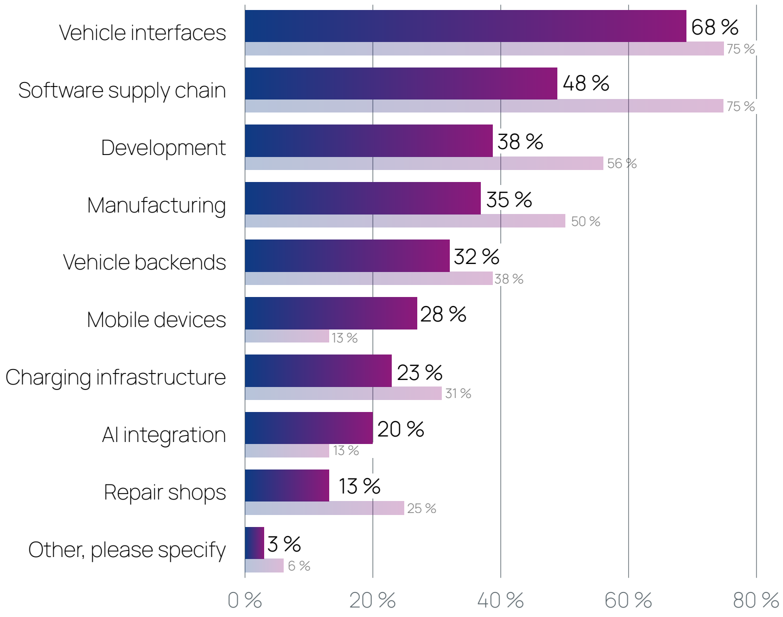
China's GB & GBT series regroups Chinese regulations and standards. If we use the same approach for European regulations, meaning regrouping the EU Cyber Resilience Act, VDA ASPICE for cybersecurity, and EU NIS 2 Directive in a single EU Framework group, and US regulations with NHTSA Cybersecurity best practices, US DoC's Securing Supply Chain, we obtain the following distribution:



8. What aspects of vehicle cybersecurity are you most concerned about?

(multiple answers)

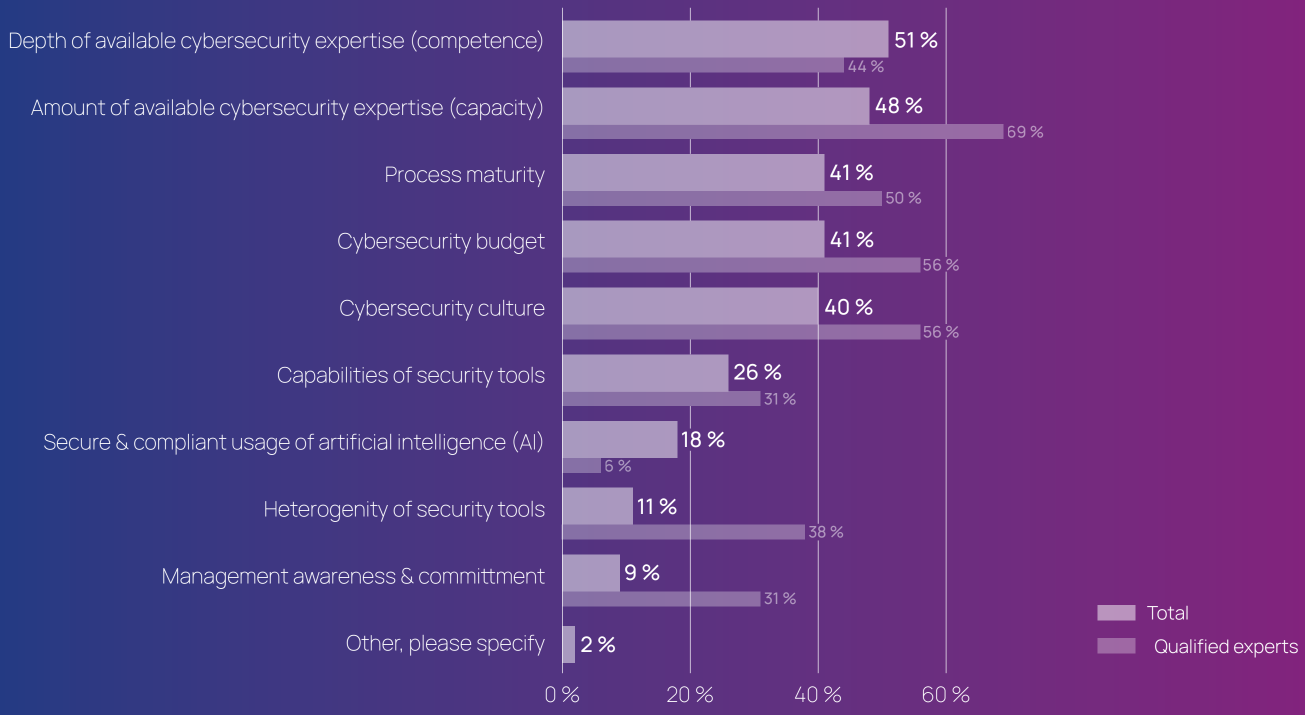
Respondents' concern with the vehicle interfaces has been consistently strong in the last three years. In the same timeframe, concern with lifecycle topics, production and software supply chain has seen the biggest increase. This trend is backed up by the view of our qualified experts.



▆ Total ▆ Qualified experts

9. What are the primary cybersecurity challenges within your area of responsibility? (multiple answers)

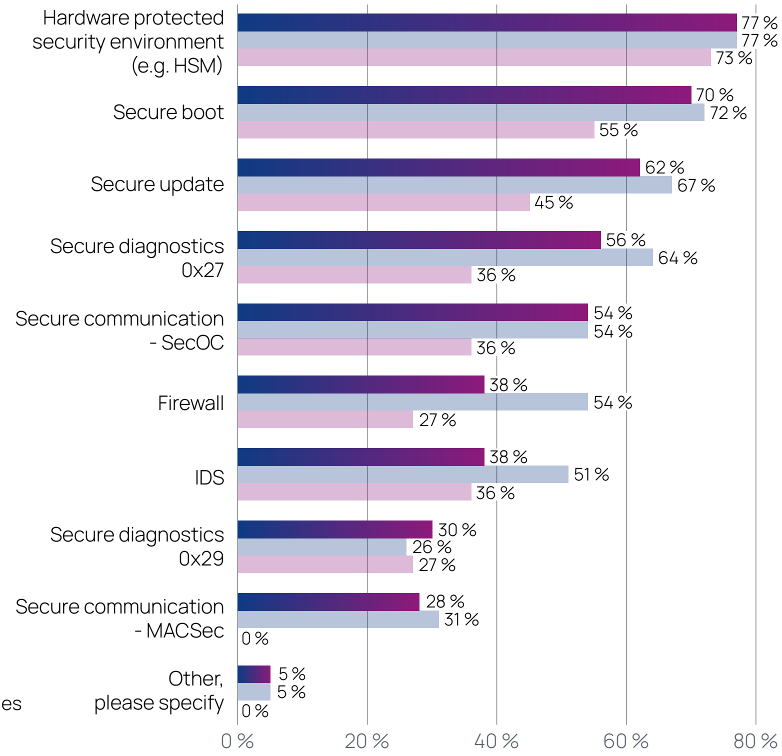
Secure and compliant usage of AI sees the biggest relative increase (from 12% to 18% over 2024 and management awareness & commitment with the largest absolute increase from 0% to 28%). Interestingly, participants in higher management positions selected the latter more often than qualified experts. Qualified experts see all challenges more often, except competence and AI.



10. What in-vehicle security measures are implemented in your company's products?

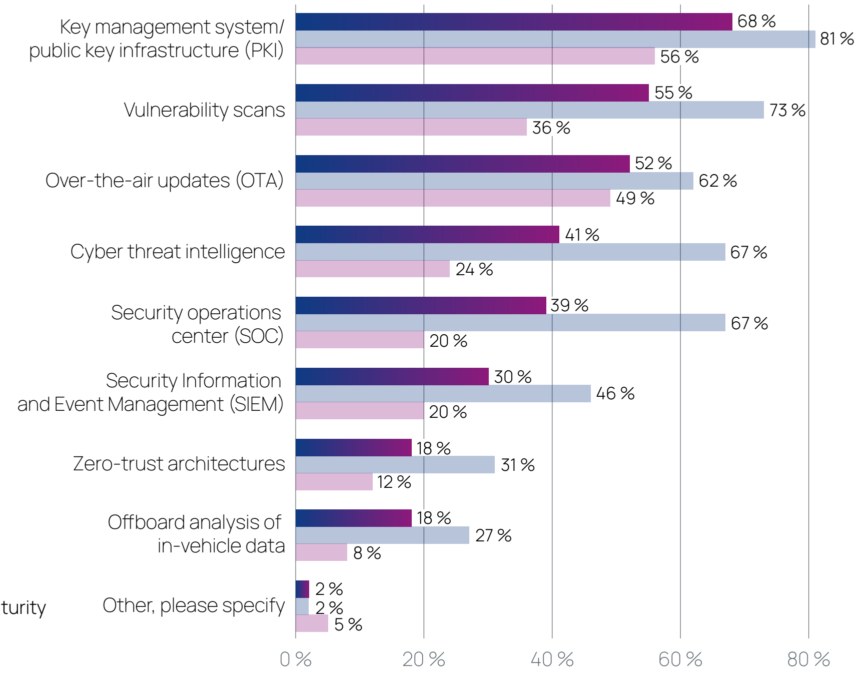
(multiple answers)

HSM deployment is prevalent both in passenger and commercial vehicles. SecOC and Secure boot are more prevalent for passenger, but conversely IDS or firewalls are more prevalent for commercial. Roughly one third of passenger vehicle respondents deploy MACSec, which could be seen as a proxy for potential SDV near-term deployment, but no respondents are deploying MACSec for commercial vehicles.



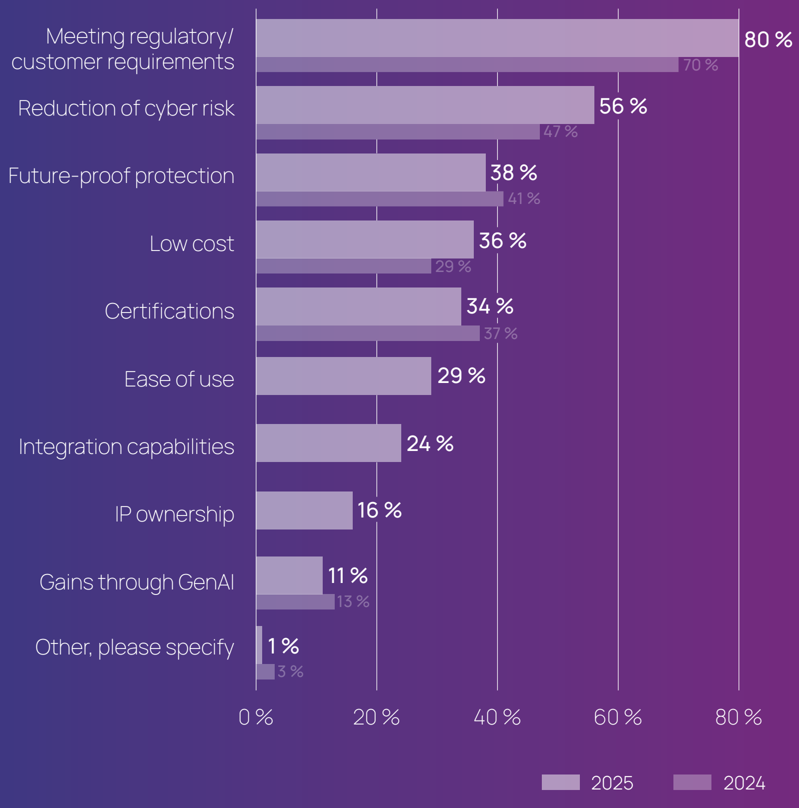
11. What additional security measures does your company implement? (multiple answers)

Key management is the most prevalent measure with almost three-quarters of automotive manufacturers adopting it. More than half of all respondents also implement OTA updates and vulnerability scans. Semiconductors are leading the zero-trust architectural charge. Higher cyber maturity correlates with higher rate of adoption for every single measure.



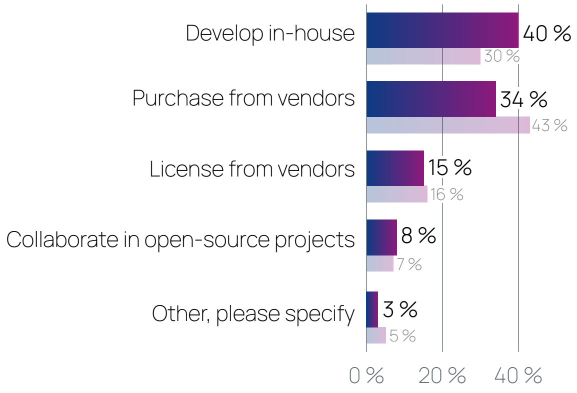
12. What are you looking most for in security solutions? (multiple answers)

Desire for low-cost solutions is trending higher than in 2024, and for the first time, lands in the top 5. Suppliers and semiconductor manufacturers mainly look to satisfy their customers, whereas commercial vehicle producers also seek certifications and risk reduction.



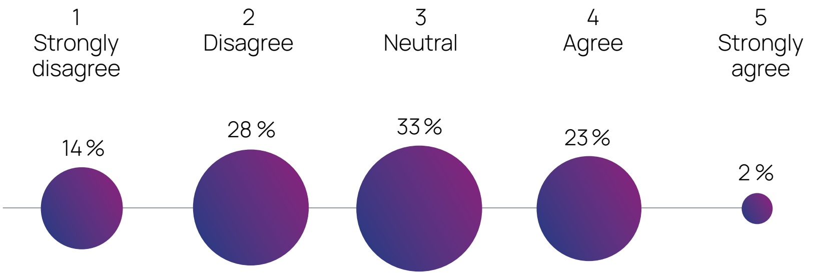
13. In your area of responsibility, what approach do you prefer for sourcing security solutions? (single answer)

About half of all respondents source solutions from vendors, with a strong preference of buy over license. As management level increases, so does the interest in turning to vendors. Collaboration in open-source projects is the least selected option for most segments (company type or size, region, cyber maturity).



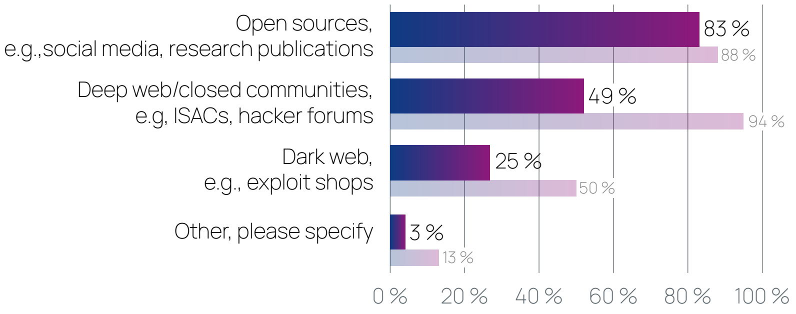
14. In your area of responsibility, do you prefer to integrate security solutions in-house or through third-parties (e.g., vendors, system integrators)? (single answer)

Suppliers and semiconductor manufacturers are most likely to integrate security solutions in-house, while passenger vehicle producers are more evenly spread on in-house or third-party integration, with a slight preference for in-house integration. In all segments, those with strong opinions prefer in-house integration of security solutions.



15. What types of sources for cyber threat intelligence do you consider in your area of responsibility? (multiple answers)

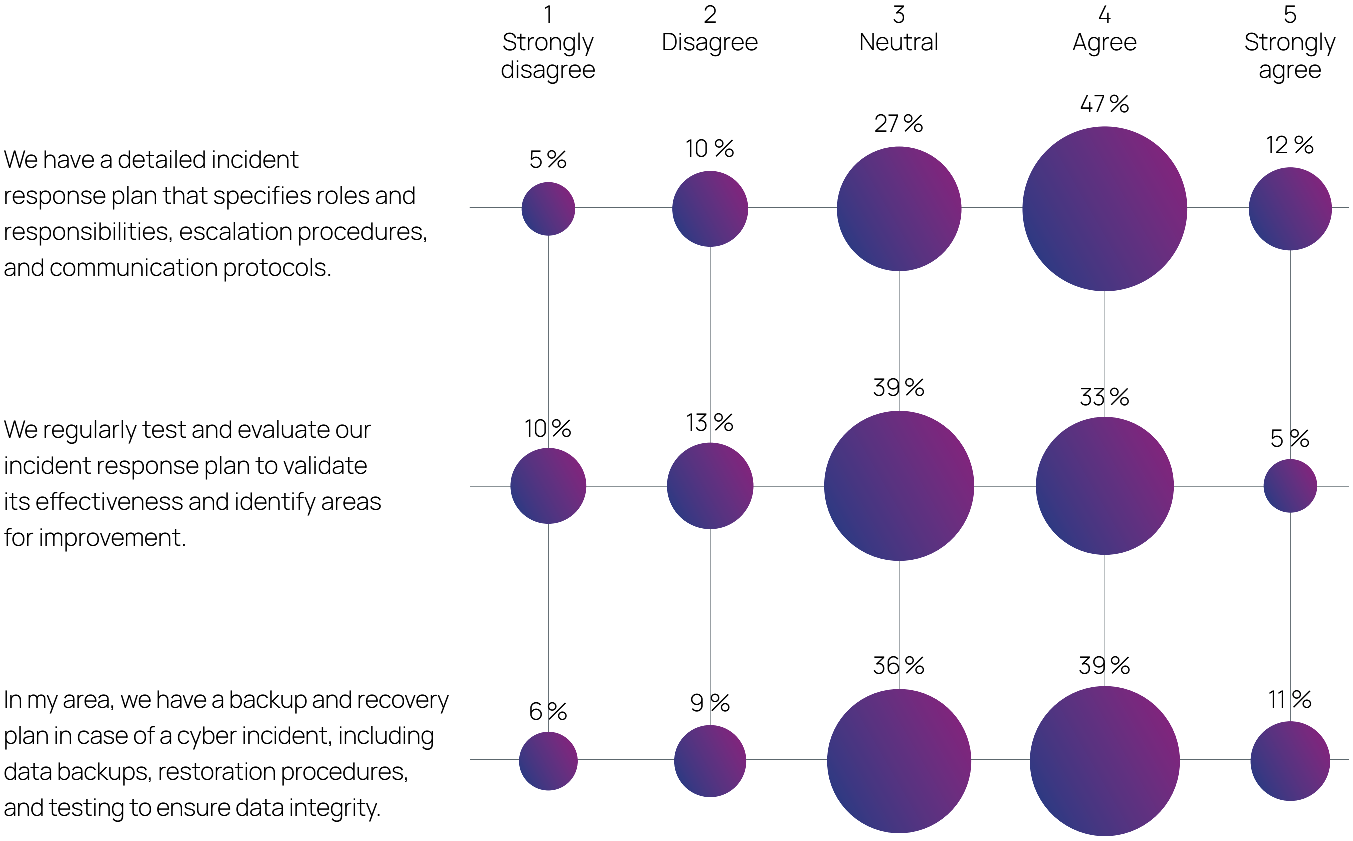
The more difficult it is to access a source, the less likely it is used for threat intelligence: Open sources score highest, followed by closed communities and the deep web and the dark web coming in last. There is a notable correlation with cyber maturity: More mature companies and qualified experts use the latter types of sources more frequently.



16. How well is your area of responsibility prepared for a cyber incident?

(single answer)

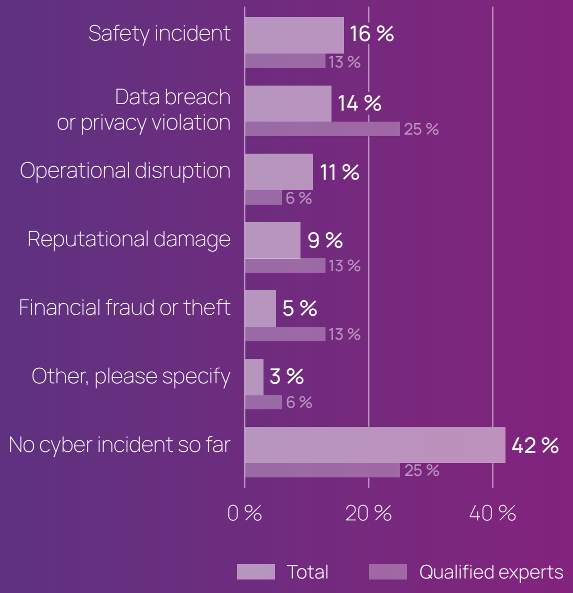
Passenger vehicle producers, and to a slightly lesser extent commercial vehicle producers, feel well prepared for cyber incidents, and regularly test them (though commercial producers not as often) and have established backup and recovery plans (again commercial vehicles less so).



17. What is the most concerning type of cyber incident that you have experienced within your area of responsibility?

(single answer)

Incidents have become commonplace as almost six out of ten participants are already aware of a cyber incident with close to 20% having observed a safety impact. This rises to 40% in China. As expected, the qualified experts have a much higher awareness of incidents with three out of four reporting an incident in their area of responsibility.

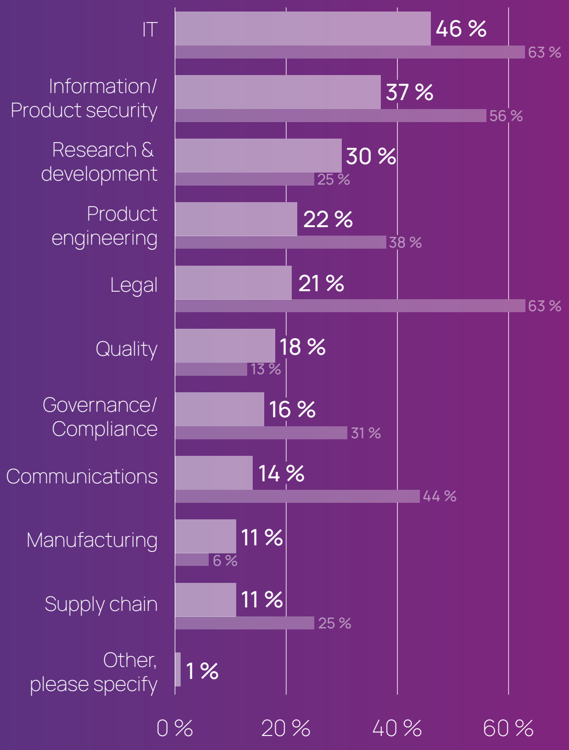


18. Regarding this cyber incident, which organizational units have been involved in its resolution?

(multiple answers)

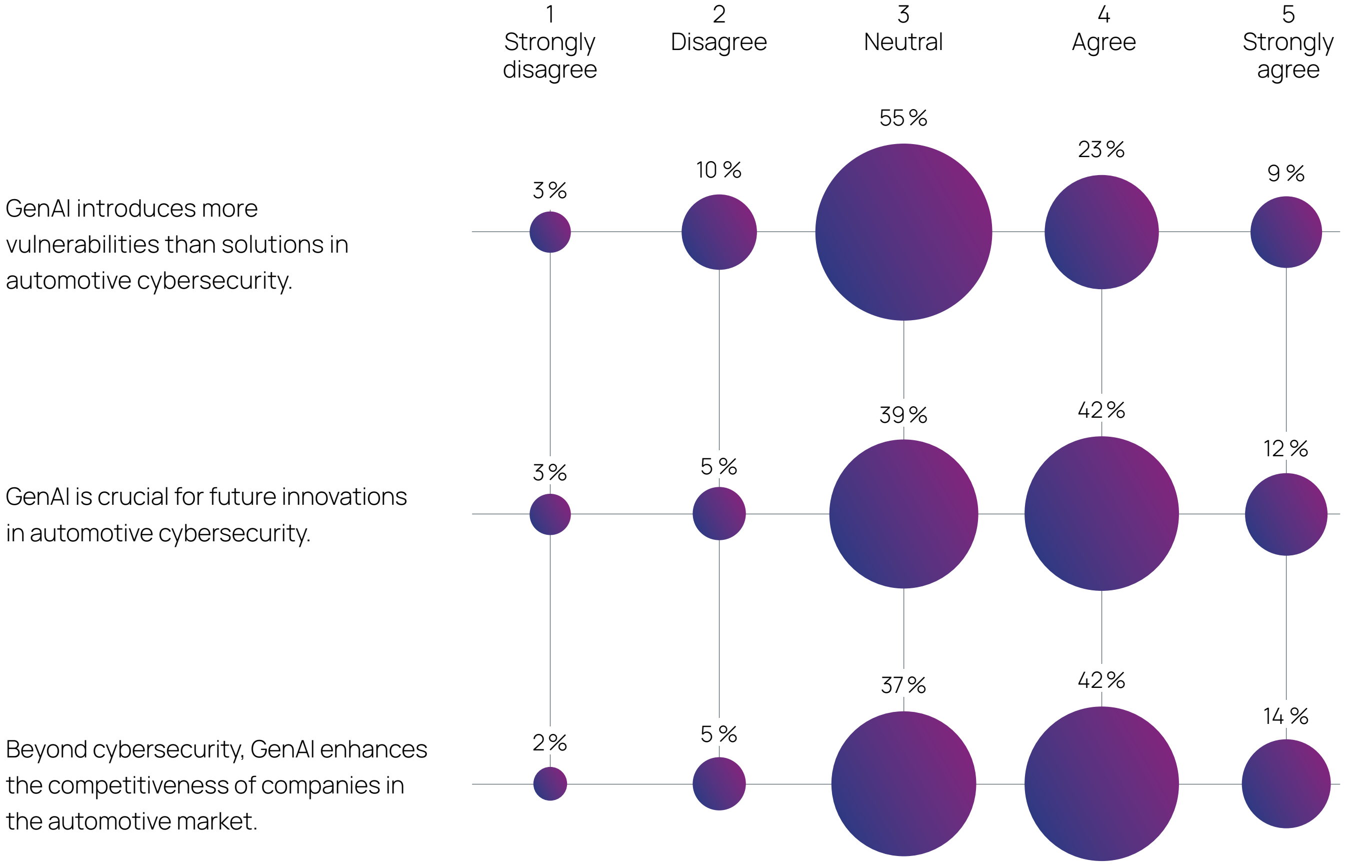
On average, participants involve between two to three different units in the resolutions of an incident. Those from information or product security teams involve other units much more frequently and to a higher degree than others, and the data shows a similar increase with the qualified experts versus general professionals.

▬ Total ▬ Qualified experts



19. How would you assess the influence of Generative AI (GenAI) on automotive security? (single answer)

Generally, respondants see GenAI as more of a threat than a solution to security issues, but also crucial for future innovations in automotive security, with semiconductor manufacturers slightly more negative, automotive suppliers more positive and vehicle producers more neutral.



Contacts & Acknowledgements

Dr. Teresina Herb	**Michael Klinger**	**Dr. Robert Lambert**	**Dr. Moritz Minzlaff**
Product Field Architect	Head of Security	Cryptography Lead	Head of Professional
Offboard Security	Western Europe	Technical Officer	Security Services
teresina.herb@etas.com	michael.klinger2@etas.com	robert.lambert@etas.com	moritz.minzlaff@etas.com

The Automotive Cyber Maturity Survey 2025 is produced thanks to a collaborative effort of: Beate Boy, Yasui Go, Meike Goelder, Janina Hofer, Isabel Huang, Julien Jarboura, Taehee Kang, Dennis Kronig, Sarah Krumrein, Kevin Schmid, Anna-Lena Sentker, Rik Thomas, Marilena Wittmann, Anton Zur and many more.

Additional recognition goes to the Auto-ISAC, escar US, isits, and KSAE for sharing and promoting the survey.

All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and up-to-date information, there can be no guarantee that this information is as accurate as it was on the date it was received or that it will continue to be accurate in the future. No one should act upon this information without appropriate professional advice and without thoroughly examining the facts of the situation in question.

Last updated: 07/2025

ETAS GmbH
Borsigstraße 24, 70469 Stuttgart, Germany
T +49 711 3423-0, info@etas.com