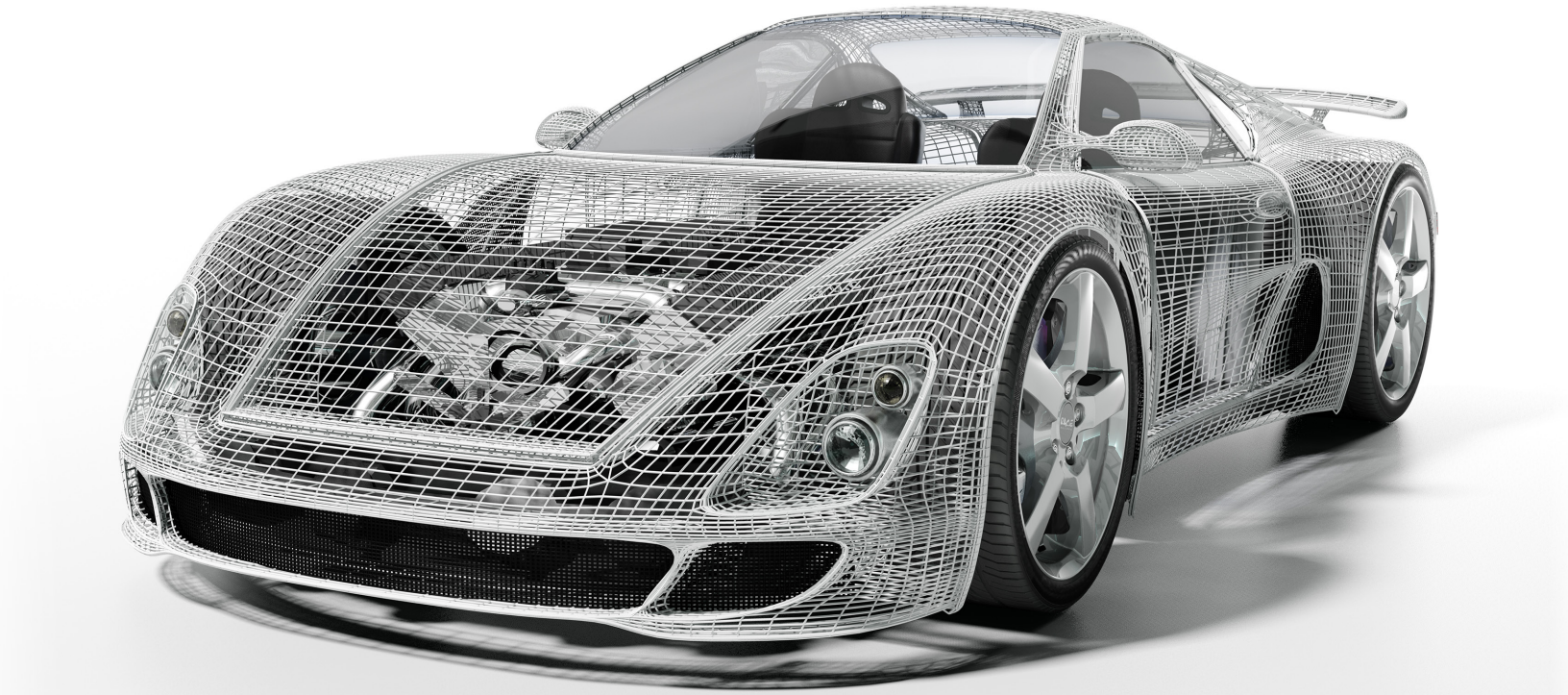
Ponemon INSTITUTE

Securing the Modern Vehicle:

A Study of Automotive Industry Cybersecurity Practices



An independent study commissioned by

SAE INTERNATIONAL™ and SYNOPSYS®

Table of Contents

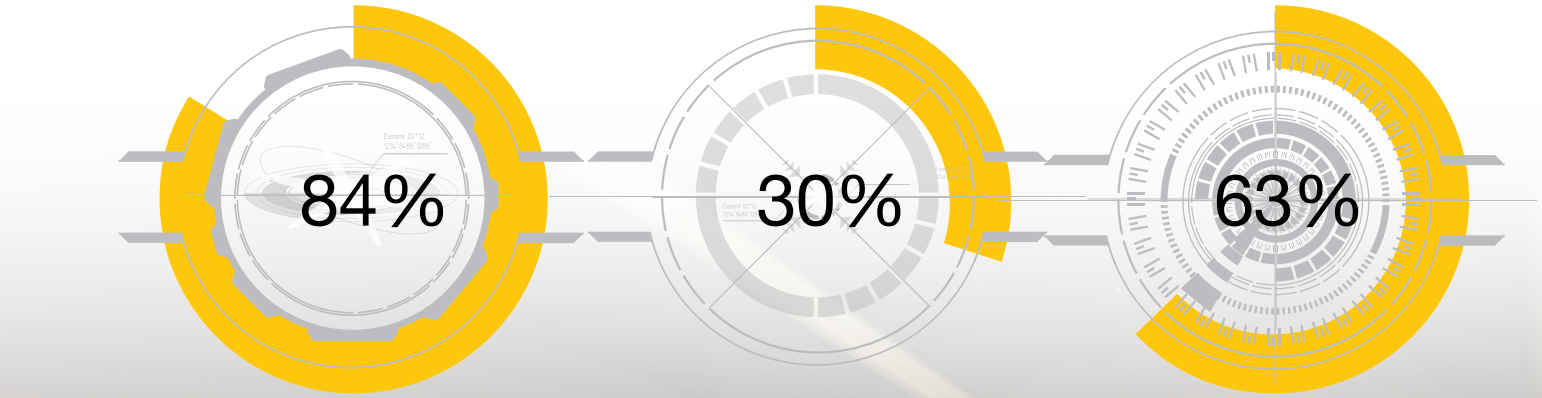
Executive Summary

Today's vehicle is a connected, mobile computer, which has introduced an issue the automotive industry has little experience dealing with: cybersecurity risk. Automotive manufacturers have become as much software as transportation companies, facing all the challenges inherent to software security.

Synopsys and SAE International partnered to commission this independent survey of the current cybersecurity practices in the automotive industry to fill a gap that has existed far too long—the lack of data needed to understand the automotive industry's cybersecurity posture and its capability to address software security risks inherent in connected, software-enabled vehicles. Ponemon Institute was selected to conduct the study. Researchers surveyed 593 professionals responsible for contributing to or assessing the security of automotive components.

Software Security Is Not Keeping Pace with Technology in the Auto Industry

When automotive safety is a function of software, the issue of software security becomes paramount—particularly when it comes to new areas such as connected vehicles and autonomous vehicles. Yet, as this report demonstrates, both automobile OEMs and their suppliers are struggling to secure the technologies used in their products. Eighty-four percent of the respondents to our survey have concerns that cybersecurity practices are not keeping pace with the ever-evolving security landscape.



have concerns that cybersecurity practices are not keeping pace with evolving technologies

do not have an established product cybersecurity program or team

test less than half of hardware, software, and other technologies for vulnerabilities

Automotive companies are still building up needed cybersecurity skills and resources. The security professionals surveyed for our report indicated that the typical automotive organization has only nine full-time employees in its product cybersecurity management program. Thirty percent of respondents said their organizations do not have an established product cybersecurity program or team. Sixty-three percent of respondents stated that they test less than half of hardware, software, and other technologies for vulnerabilities.

Pressure to meet product deadlines, accidental coding errors, lack of education on secure coding practices, and vulnerability testing occurring too late in production are some of the most common factors that render software vulnerabilities. Our report illustrates the need for more focus on cybersecurity; secure coding training; automated tools to find defects and security vulnerabilities in source code; and software composition analysis tools to identify third-party components that may have been introduced by suppliers.

Software in the Automotive Supply Chain Presents a Major Risk

While most automotive manufacturers still produce some original equipment, their true strength is in research and development, designing and marketing vehicles, managing the parts supply chain, and assembling the final product. OEMs rely on hundreds of independent vendors to supply hardware and software components to deliver the latest in vehicle technology and design.

Seventy-three percent of respondents surveyed in our report say they are very concerned about the cybersecurity posture of automotive technologies supplied by third parties. However, only 44 percent of respondents say their organizations impose cybersecurity requirements for products provided by upstream suppliers.

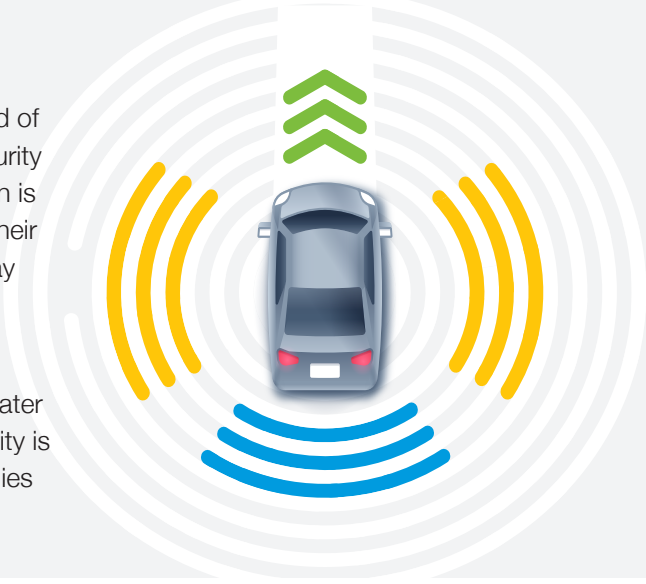
Connected Vehicles Offer Unique Security Issues

Automakers and their suppliers also need to consider what the connected vehicle means for consumer privacy and security. As more connected vehicles hit the roads, software vulnerabilities are becoming accessible to malicious hackers using cellular networks, Wi-Fi, and physical connections to exploit them. Failure to address these risks might be a costly mistake, including the impact they may have on consumer confidence, personal privacy, and brand reputation.

Respondents to our survey viewed the technologies with the greatest risk to be RF technologies (such as Wi-Fi and Bluetooth), telematics, and self-driving (autonomous) vehicles. This suggests non-critical systems and connectivity are low-hanging fruit for attacks and should be the main focus of cybersecurity efforts.

Conclusion

As will be clear in the following pages, survey respondents in a myriad of sectors of the industry show a significant awareness of the cybersecurity problem and have a strong desire to make improvements. Of concern is the 69 percent of respondents who do not feel empowered to raise their concerns up their corporate ladder, but efforts such as this report may help to bring the needed visibility of the problem to the executive and boardroom level.



Just as lean manufacturing and ISO 9000 practices both brought greater quality to the automotive industry, a rigorous approach to cybersecurity is vital to achieve the full range of benefits of new automotive technologies while preserving quality, safety, and rapid time to market.

Organizational Dynamics and Challenges

Even though they see a clear danger, respondents do not feel they can raise their concerns about cybersecurity to upper management.

Sixty-two percent of those surveyed say a malicious or proof-of-concept attack against automotive technologies is likely or very likely in the next 12 months, but 69 percent reveal that they do not feel empowered to raise their concerns up their chain of command.

As shown in Figure 1, more than half (52 percent) of respondents are aware of potential harm to drivers of vehicles because of insecure automotive technologies, whether developed by third parties or by their organizations. However, only 31 percent say they feel empowered to raise security concerns within their organizations.

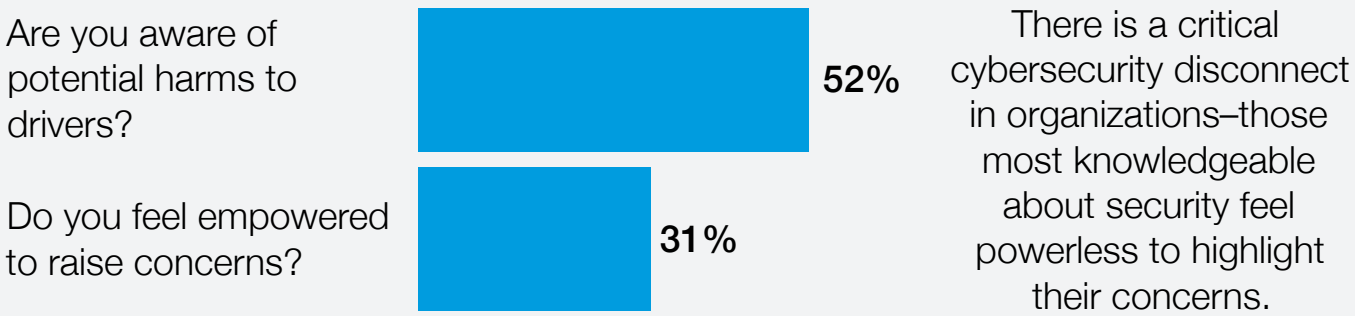


Figure 1. Awareness of potential harms to drivers exists but concerns are not voiced. "Yes" responses presented

Despite those concerns, there is a lack of product cybersecurity teams and programs.

In your opinion, how likely is a malicious or proof-of-concept (i.e. security research) attack to occur against automotive software/technology/components developed or in use by your organization over the next 12 months?	• ***Very likely***	***27%***
	• ***Likely***	***35%***
	• Somewhat likely	23%
	• Not likely	15%

Do you feel empowered to raise concerns about the security of automotive technology in your organization?	• Yes	31%
	• ***No***	***69%***

Thirty percent of respondents overall say their organizations do not have an established product cybersecurity program or team. Only 10 percent say their organizations have a centralized product cybersecurity team that guides and supports multiple product development teams.

Which of the following best describes your organization's approach to product cybersecurity? Please select one choice only.	• Product cybersecurity is part of the traditional IT cybersecurity team (typically under a global CISO)	20%
	• Product cybersecurity is part of the functional safety team	17%
	• We have a centralized product cybersecurity team (i.e. center of excellence) that guides and supports multiple product development teams	10%
	• We have a decentralized product cybersecurity team, with cybersecurity experts attached to specific product development teams	23%
	• ***We do not have an established product cybersecurity program or team***	***30%***

When these data are broken down by OEM or supplier (Figure 2), 41 percent of respondents in suppliers do not have an established product cybersecurity program or team of any kind. In contrast, only 18 percent of OEMs do not have a product security program or team.

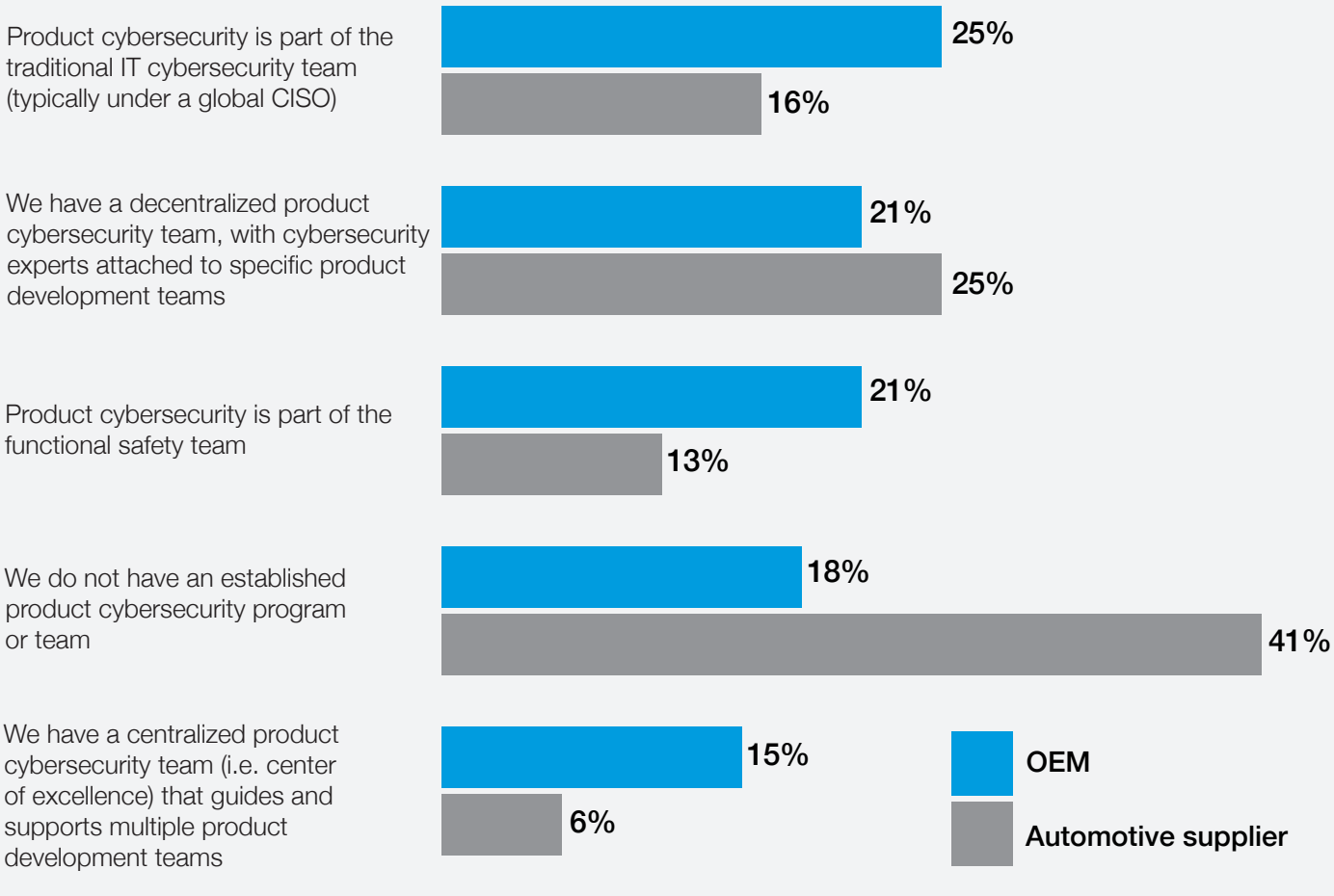


Figure 2. Which of the following describes your organization's approach to product cybersecurity?

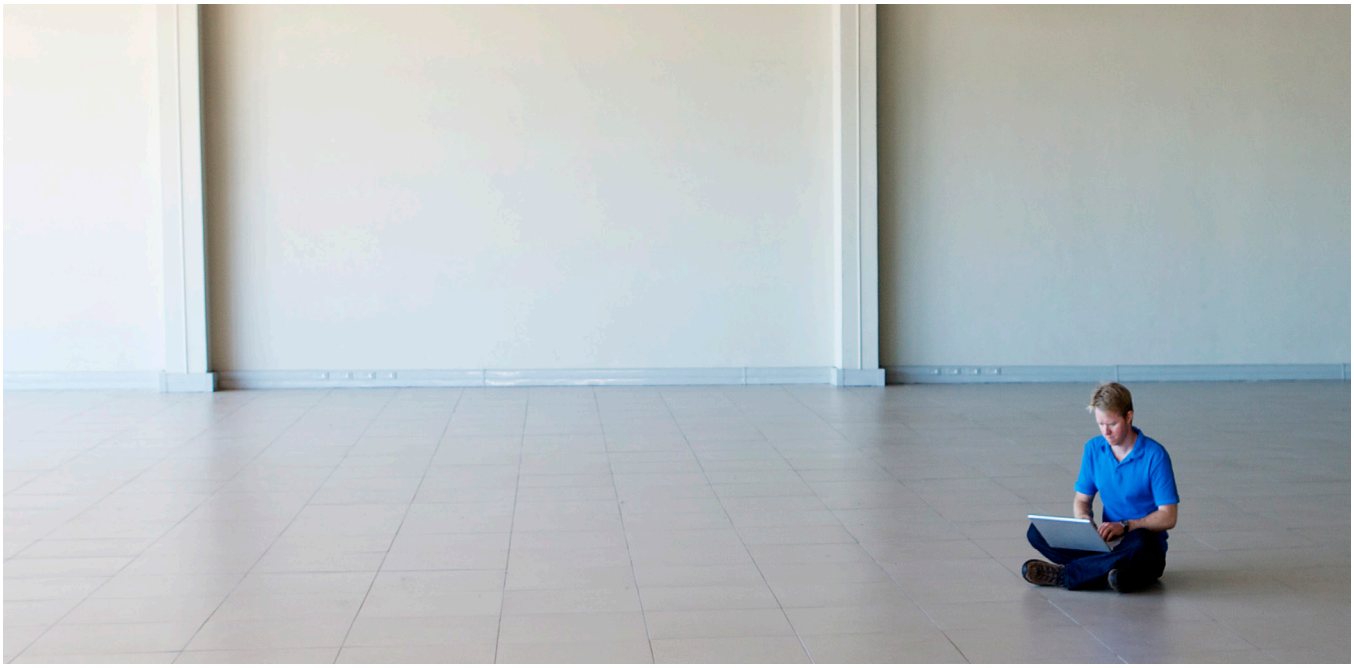
A significant percentage of suppliers are overlooking a well-established best practice: to employ a team of experts to conduct security testing throughout the product development process, from the design phase through decommissioning.

Automotive companies lack necessary cybersecurity resources and skills.

The majority of the industry respondents believe they do not have appropriate levels of resources to combat the cybersecurity threats in the automotive space.

On average, companies have only nine full-time employees in their product cybersecurity management programs. Sixty-two percent of respondents say their organizations do not have the necessary cybersecurity skills. More than half (51 percent) say they do not have enough budget and human capital to address cybersecurity risks.

Does your organization allocate enough resources (i.e. budget and human resources) to cybersecurity?	• Yes	49%
	• ***No***	***51%***
Does your organization have the necessary cybersecurity skills in product development?	• Yes	38%
	• ***No***	***62%***
How many FTEs participate in product cybersecurity management programs in your organization?	• ***Less than 5***	***30%***
	• ***5 to 10***	***44%***
	• ***11 to 20***	***18%***
	• More than 20	8%



Technical Dynamics and Challenges

Vehicles are now essentially a mobile IT enterprise that includes control systems, rich data, infotainment, and wireless mesh communications through multiple protocols. That connectivity can extend to the driver's personal electronic devices, to other vehicles and infrastructure, and through the Internet to OEM and aftermarket applications, making them targets for cyberattacks. Unauthorized remote access to the vehicle network and the potential for attackers to pivot to safety-critical systems puts at risk not just drivers' personal information but their physical safety as well.

Automotive engineers, product developers, and IT professionals highlighted several major security concern areas as well as security controls they use to mitigate risks.

A majority (84 percent) of respondents are concerned that cybersecurity practices are not keeping pace with changing technology.

How concerned are you that your organization's cybersecurity practices are not keeping pace with changing automotive technologies? 1 = not concerned to 10 = very concerned	• 1 or 2	5%
	• 3 or 4	11%
	• ***5 or 6***	***25%***
	• ***7 or 8***	***22%***
	• ***9 or 10***	***37%***

Technologies viewed as causing the greatest risk are RF technologies, telematics, and self-driving vehicles. Of the technological advances making their way into vehicles, these three are seen to pose the greatest cybersecurity risks. Organizations should be allocating a larger portion of their resources to reducing the risk in these technologies.

Respondents say that pressure to meet product deadlines (71 percent), lack of understanding/training on secure coding practices (60 percent), and accidental coding errors (55 percent) are the most common factors that lead to vulnerabilities in their technologies. Engaging in secure coding training for key staff will target two of the main causes of software vulnerabilities in vehicles.

Which technologies pose the greatest cybersecurity risk? Select all that apply.	• Infotainment systems	31%
	• Powertrain control units	46%
	• SOC system on chip-based components	44%
	• ***Self-driving (autonomous) vehicles***	***58%***
	• Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)	51%
	• ***Telematics***	***60%***
	• Steering systems	45%
	• Electrification components	17%
	• Cameras	29%
	• ***RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)***	***63%***

What are the primary factors that lead to vulnerabilities in the automotive technologies developed or in use by your organization. Select the top four factors.	• ***Accidental coding errors***	***55%***
	• The use of insecure/outdated open source software components	40%
	• Malicious code injection	23%
	• Lack of internal policies or rules that clarify security requirements	26%
	• ***Lack of understanding/training on secure coding practices***	***60%***
	• ***Pressure to meet product deadlines***	***71%***
	• Lack of quality assurance and testing procedures	50%
	• Product development tools have inherent bugs	39%
	• Incorrect permissions	19%
	• Back end systems	15%

Security patches and updates are a challenge.

Only 39 percent of respondents say their software update delivery model addresses critical security vulnerabilities in a timely manner.

Does your organization's software update delivery model address critical security vulnerabilities in a timely manner?	• Yes	39%
	• ***No***	***61%***

As shown in Figure 3, 65 percent say security patches and updates for vehicles in-market are delivered through procured software, components, and systems. Fifty-one percent say this happens through wireless communications connected to personal electronic/computing devices.

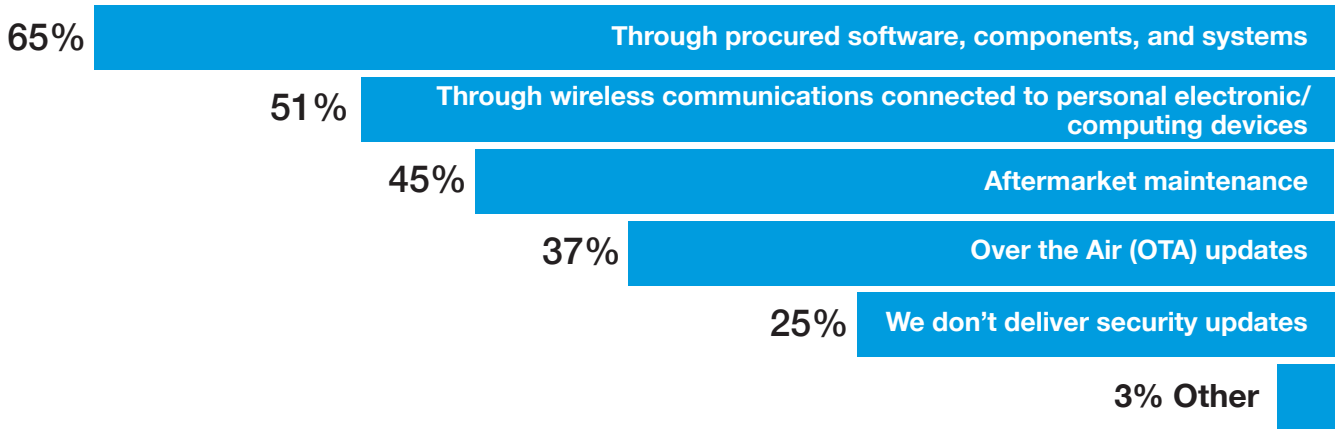


Figure 3. How does your organization deliver security patches and updates for vehicles in-market?

Only 37 percent say they use over-the-air (OTA) updates to deliver security patches, but more than 50 percent say they will do so in the next 5 years. This suggests the need for an industry standard for secure OTA updates.

If you don't deliver OTA updates, do you plan to in the future?	
• ***Yes, in 1 to 3 years***	***33%***
• ***Yes, in 3 to 5 years***	***23%***
• ***Greater than 5 years***	***9%***
• No plans to deliver OTA updates	35%

Firewalls and gateways are the most common security controls incorporated into vehicles.

Sixty-four percent of respondents incorporate firewalls and 59 percent use gateways as key security controls.

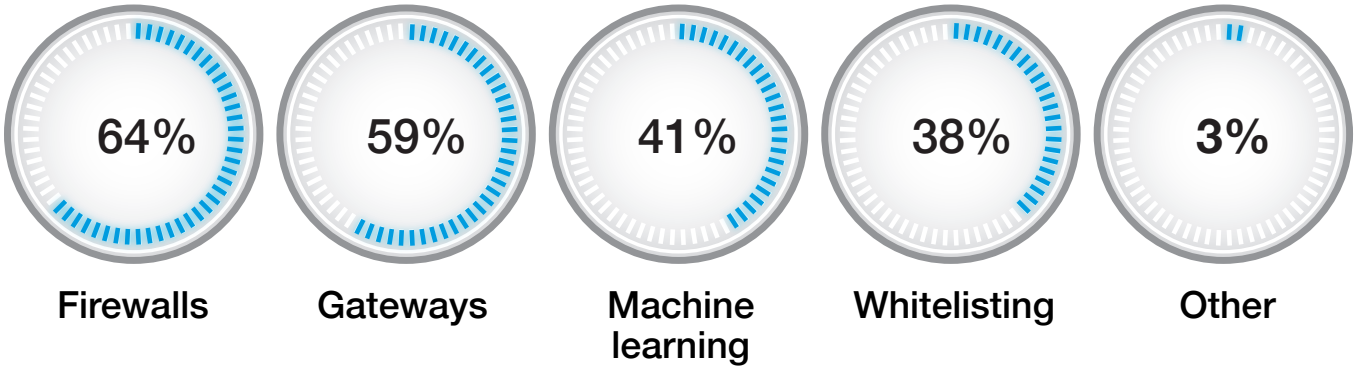


Figure 4. Does your organization incorporate security counter measures in its vehicles?

A majority of companies use key management systems, but 43 percent still use a manual process.

Sixty-three percent of respondents say their organizations use key management systems (the management of cryptographic keys, including generation, exchange, storage, use, and replacement of keys). As shown in Figure 5, 56 percent use a central key management system/server while 45 percent have a formal key management policy. Yet 43 percent use a manual process for key management, limiting its usefulness and hampering security.

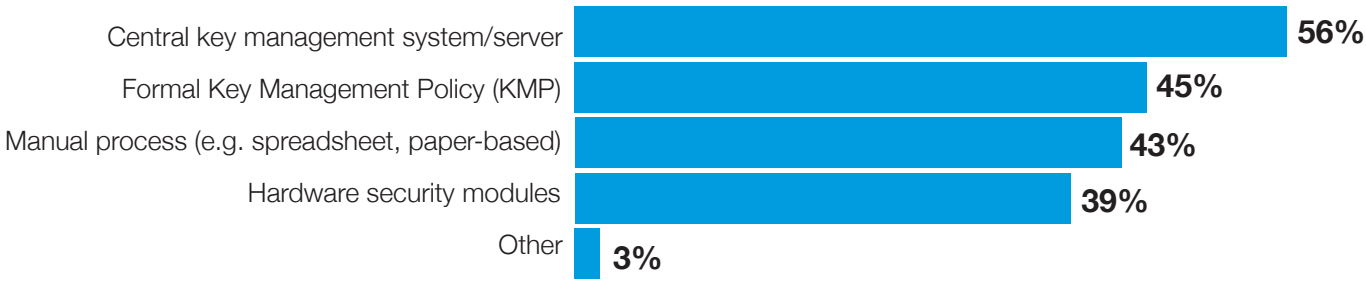


Figure 5. What key management systems does your organization presently use?

Product Development and Security Testing Practices

Our survey questions targeted the security practices that companies employ in their product development. An established best practice is to use a risk-based, process-driven approach to cybersecurity, integrating it into the entire product development life cycle.

The survey found security vulnerabilities are being assessed far too late in the product release process.

Only 47 percent of companies assess vulnerabilities in the *requirements and design* phase or the *development and testing* phase (see Figure 6).

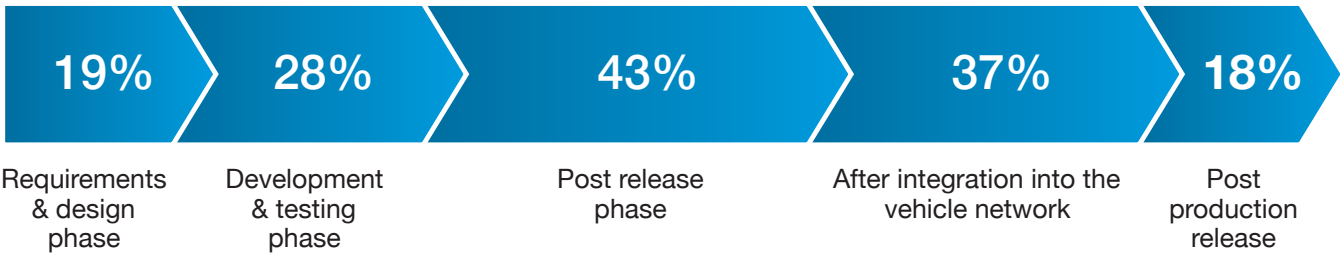


Figure 6. When during the development life cycle does your organization assess automotive software/technology/components for security vulnerabilities?

This process is contrary to the guidance of SAE J3061™ *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,*[1] which advocates for a risk-based, process-driven approach to cybersecurity throughout the entire product development life cycle.

Advantages of Integrating Security into Product Development

1. Integrating security concepts into product design achieves higher security than applying security controls post production.
2. Risks and vulnerabilities are identified early, and appropriate security controls can be applied.
3. This is a vastly more efficient way to apply limited cybersecurity resources and normalizes cybersecurity costs as a critical piece of the product development discipline.

J3061 is the world's first automotive cybersecurity standard, and it is a valuable tool to incorporate cybersecurity processes into product development.

[1] *SAE J3061™ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, SAE International, January 2016

Failure to perform adequate security tests leads to vulnerabilities.

Sixty-three percent of respondents state that they test less than 50 percent of hardware, software, and other technologies for vulnerabilities. Additionally, 71 percent believe that pressure to meet product deadlines is the primary factor leading to security vulnerabilities. These responses suggest that few software/technology/components are being tested in order for organizations to meet deadlines.

What percentage of automotive technology used by your organization is tested for cybersecurity vulnerabilities?	• ***None***	***25%***
	• ***Less than 25%***	***12%***
	• ***26% to 50%***	***26%***
	• 51% to 75%	23%
	• 76% to 100%	14%
	Total	100%
What negative business impacts are caused by insecure automotive technology used by your organization?	• Security-related recalls	21%
	• Damage to supply chain partner relationships	54%
	• ***Delayed or missed release dates***	***67%***
	• ***Unintended interaction between components during integration testing***	***59%***
	• Regulatory impacts, sanctions, or fines	5%
	• Not aware of any adverse events	29%
What are the primary factors leading to vulnerabilities in the automotive technologies used by your organization?	• Accidental coding errors	55%
	• The use of insecure/outdated open source software components	40%
	• Malicious code injection	23%
	• Lack of internal policies or rules that clarify security requirements	26%
	• Lack of understanding/training on secure coding practices	60%
	• ***Pressure to meet product deadlines***	***71%***
	• Lack of quality assurance and testing procedures	50%
	• Product development tools have inherent bugs	39%
	• Incorrect permissions	19%
	• Back end systems	15%

The pressure to meet deadlines leads to inadequate security testing, which causes the very vulnerabilities that companies seek to avoid.

Vulnerabilities and quality issues are a result of the lack of consistent use of secure software development life cycle (SSDLC) practices.

Over 33 percent of the industry is not using accepted SSDLC practices, and 60 percent say their companies have a lack of understanding or training on secure coding practices.

Does your organization follow an internally or externally published Secure Software Development Life Cycle (SDLC) process for automotive software/technology/components?		
	• Yes, internally	35%
	• Yes, externally	29%
	• ***No***	***36%***

Sixty percent of respondents say a lack of understanding/training on secure coding practices leads to vulnerabilities in automotive software/technology/components. Fifty-five percent cite accidental coding errors.

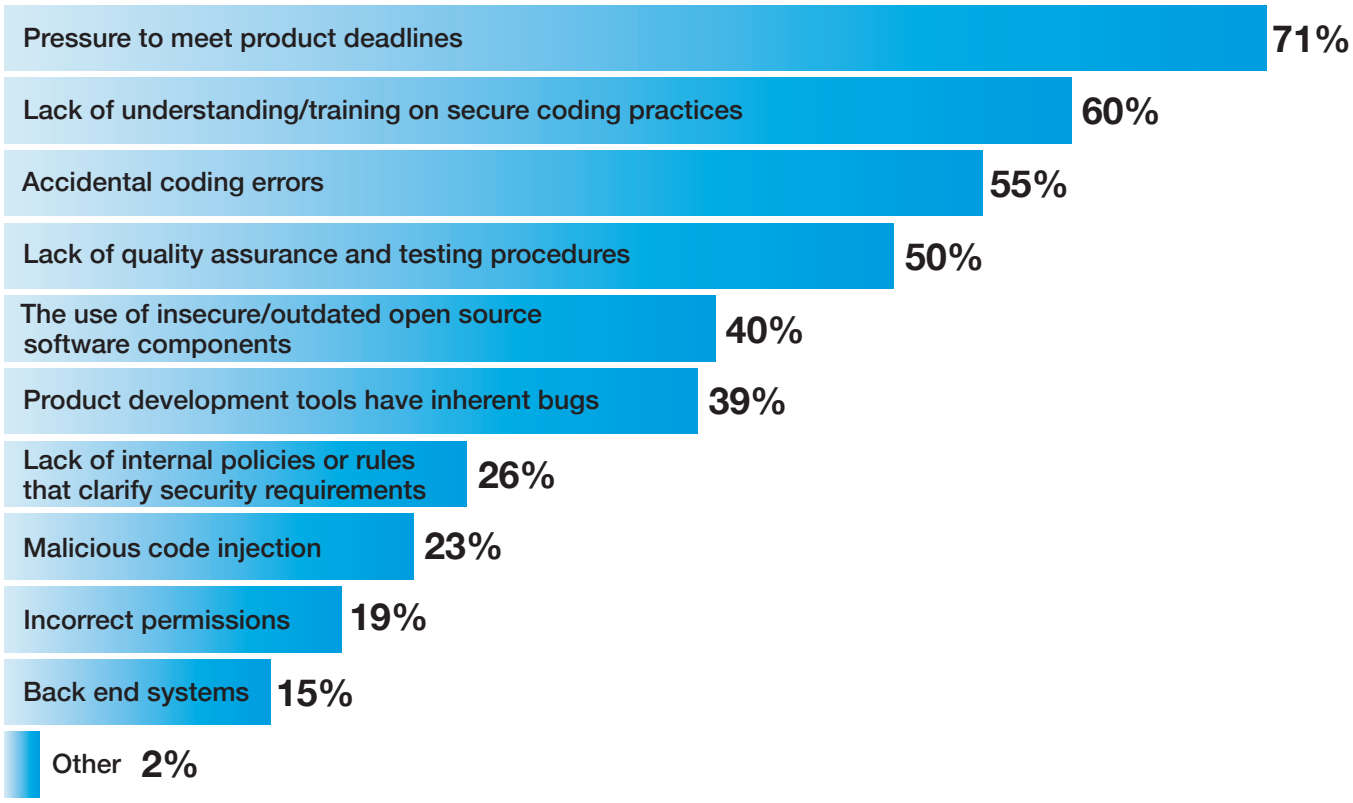


Figure 7. What are the primary factors that lead to vulnerabilities in automotive software/technology/components?

The industry's most common security activities are security patch management, penetration testing, and dynamic security testing (DAST).

Respondents state the most common techniques to secure automotive technologies are security patch management (61 percent), penetration testing (56 percent), and dynamic security testing/DAST (49 percent). Interestingly, these are all techniques used at later stages of the life cycle.

This is another illustration of the general theme that cybersecurity is not being fully integrated throughout the system development life cycle—in particular, at the early requirements, design, and testing and development phases.

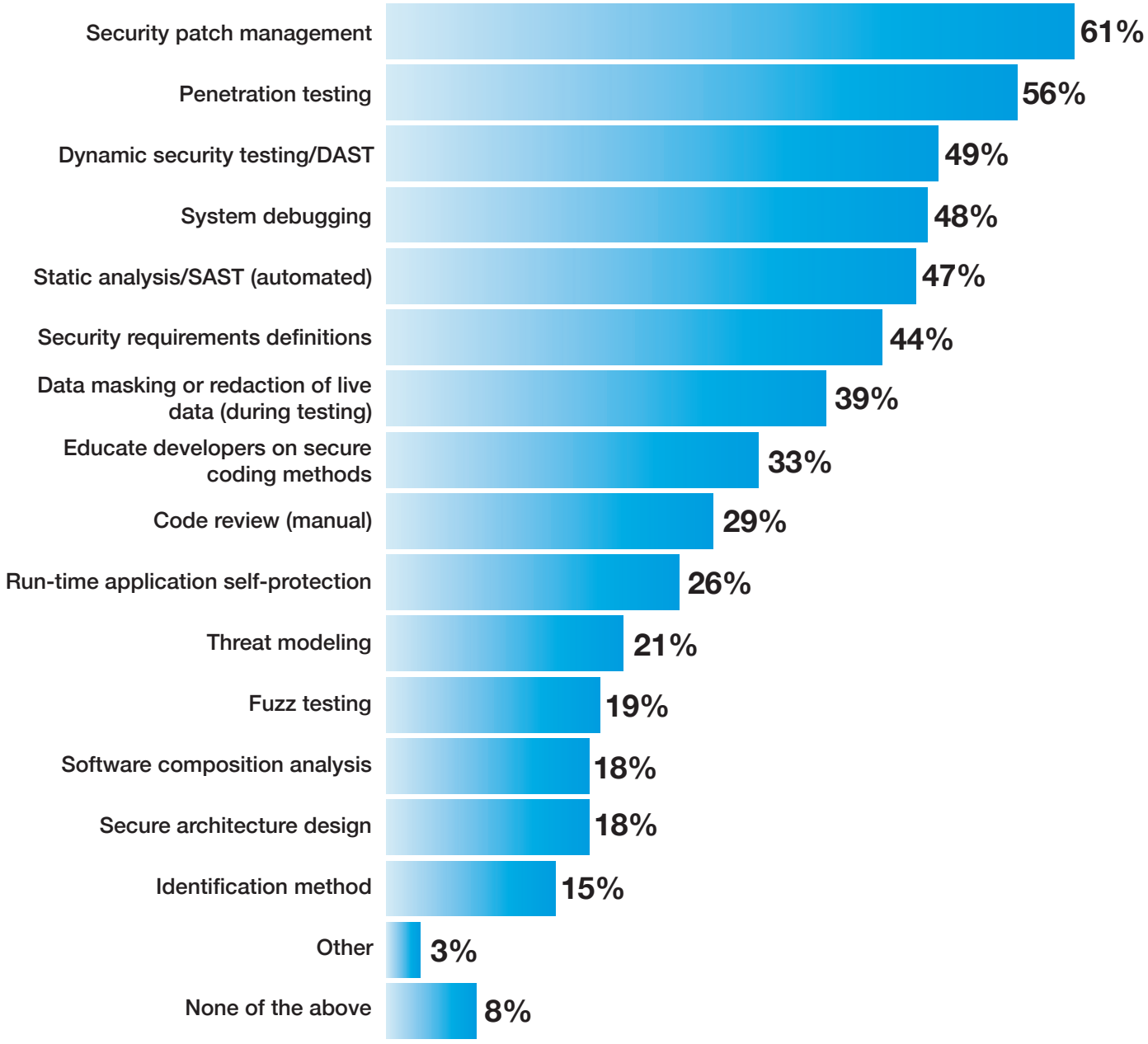


Figure 8. What activities does your company use to secure automotive software/technology/components?

Supply Chain and Third-Party Component Challenges

The automotive industry's complex and disparate supply chain is a major culprit in causing quality issues rendering security vulnerabilities. The frequent integration of third-party components, software, communications protocols, and applications often introduces threat vectors that OEMs must address. Several key takeaways are related to these factors.

Vulnerabilities in the automotive supply chain present a major risk.

Seventy-three percent of respondents are very concerned about the cybersecurity posture of automotive technologies supplied by third parties. Sixty-eight percent are also very concerned about the cybersecurity posture of the industry as a whole.

Only 44 percent say their organizations impose cybersecurity requirements for products provided by upstream suppliers. A target initiative for manufacturers should be to develop appropriate security requirements along with other technical requirements for suppliers' software, hardware, and systems.

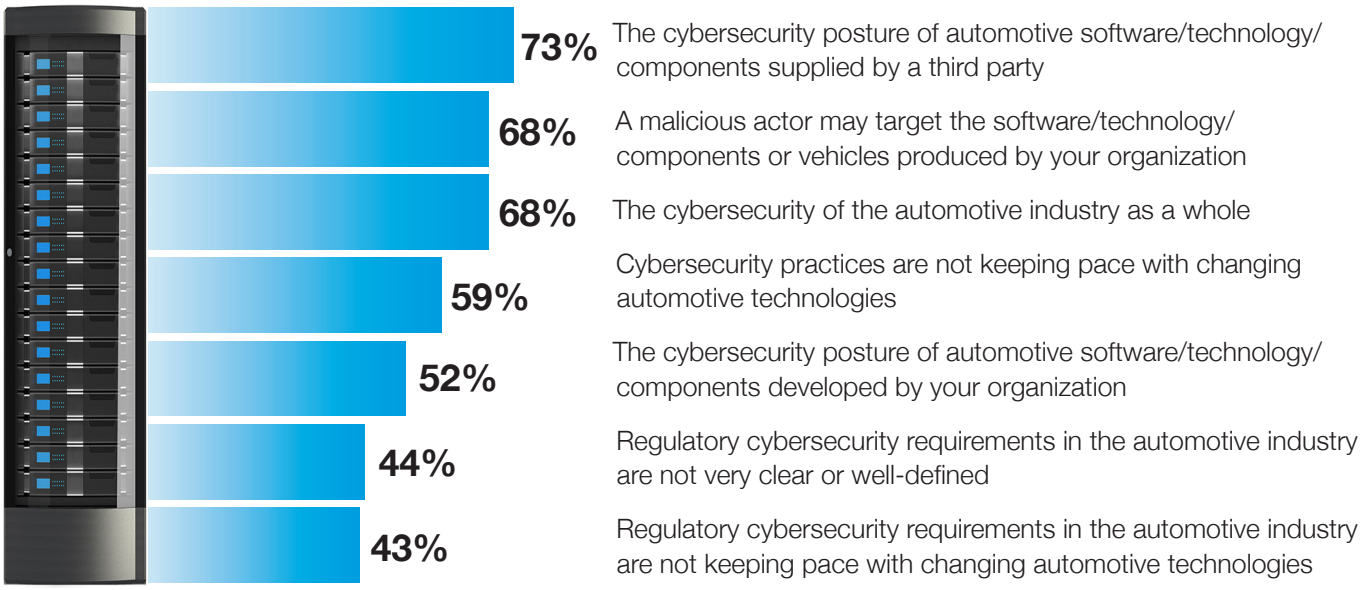


Figure 9. Very high concerns about cybersecurity practices and posture
1 = not concerned to 10 = very concerned, 7+ responses presented

Education on secure coding methods is not being prioritized.

Only 33 percent of respondents say their organizations educate developers on secure coding methods. Sixty percent say a lack of understanding or training on secure coding practices is a primary factor that leads to vulnerabilities.

What activities does your organization employ to secure automotive software/technology/components?	• ***Educate developers on secure coding methods***	***33%***

Conclusions

Survey respondents show a significant awareness of the cybersecurity challenges facing them and a desire to improve, tempered by concerns that they do not feel empowered to raise these issues to senior management. Respondents have an excellent understanding of perhaps the most important tenet of the cybersecurity discipline: engaging in cybersecurity throughout product development.

Finding the right combination of people, processes, and technology is the key to success. Solutions exist to deepen the ability of security professionals currently engaged in security initiatives as well as those new to the process of developing an efficient and effective approach to security, such as these resources:

- SAE J3061™ *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* describes a cybersecurity process framework from which an organization can develop an internal cybersecurity process to design and build cybersecurity into vehicle systems.
- The National Institute of Science and Technology (NIST) is a valuable and free resource for security knowledge and best practices (e.g. the NIST Special Publication 800 series).
- The Building Security In Maturity Model (BSIMM) and the Synopsys Automotive Security resource page can help organizations develop a security initiative and meet security, safety, reliability, and compliance requirements for automotive software.

These solutions advocate developing and utilizing a risk-based, process-driven approach that binds cybersecurity to the entire product development life cycle and the secure software development life cycle.

Cybersecurity training is also a critical investment that not only targets one pain point respondents shared in the survey but also pays dividends far into the future, helping to build a culture of security throughout an enterprise.

The automotive industry also has resources to enhance knowledge of emerging security issues and trends, develop professional networks, and contribute to industry-wide security.

- The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a valuable forum for security professionals to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance automotive industry cybersecurity.
- SAE International has several cybersecurity groups developing standards, guidelines, and best practices, provides professional development training, and hosts conferences and events to keep the industry abreast of the state of the practice.

The concerns about supply chain risks noted in this report can be addressed or even mitigated by paying close attention to the requirements phase of the development life cycle. This may involve working closely with suppliers to identify weaknesses in the design or architecture of relevant components. Additional assurances can be achieved by conducting periodic reviews of suppliers' cybersecurity processes or imposing cybersecurity assurance requirements on supplier agreements.

Cybersecurity shouldn't be viewed as a cost center and tacked on at the end of production, but instead should be programmed into every step of the systems engineering process that guides the entire product development life cycle—notably, the secure software development life cycle (SSDLC). Automotive companies can enjoy a wide range of solutions through guidance, best practices, and standards that have already been developed in other industries.

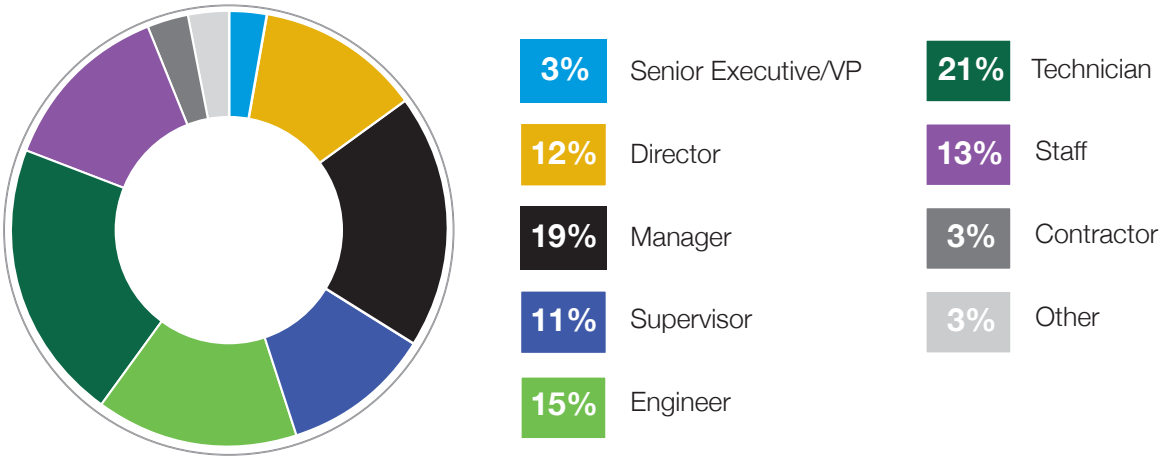
This rigorous approach to cybersecurity is vital to achieve enhanced safety while ensuring security, quality, and rapid time to market.

Methods

A sampling frame of 15,900 IT security practitioners and engineers in the automotive industry were selected as participants in this survey. To ensure knowledgeable responses, all respondents are involved in contributing to or assessing the security of an automotive component. Table 1 shows 677 total returns. Screening and reliability checks required the removal of 84 surveys. Our final sample consisted of 593 surveys, or a 3.7 percent response rate.

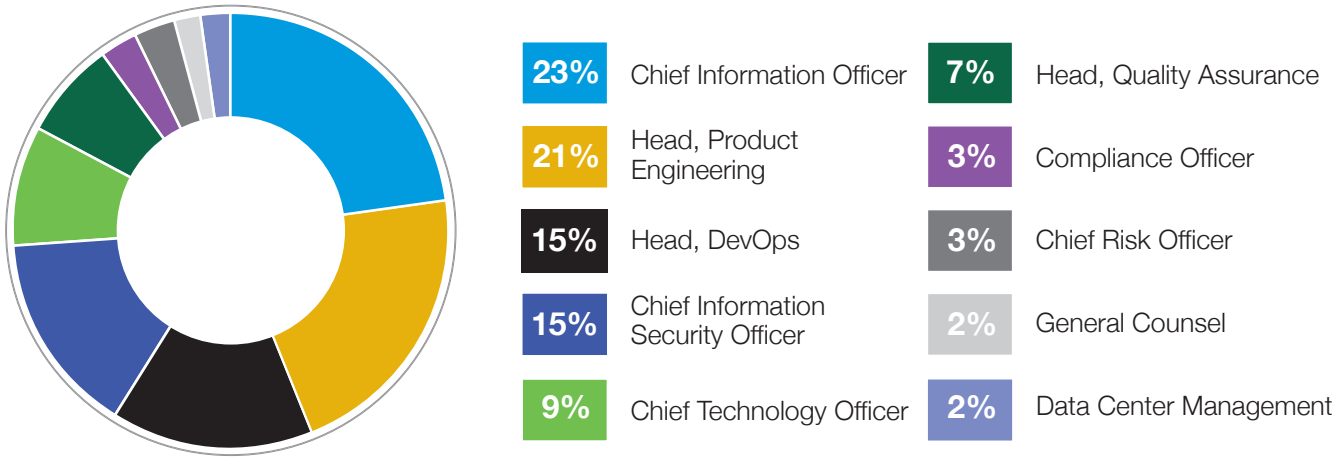
Table 1. Sample response	**Freq.**	**Pct%**
• Total sample frame	15,900	100.0%
• Total returns	677	4.3%
• Rejected surveys	84	0.5%
• Final sample	593	3.7%

Pie Chart 1 reports the respondents' position in participating organizations. By design, more than half (60 percent) hold engineer or higher-ranked positions.



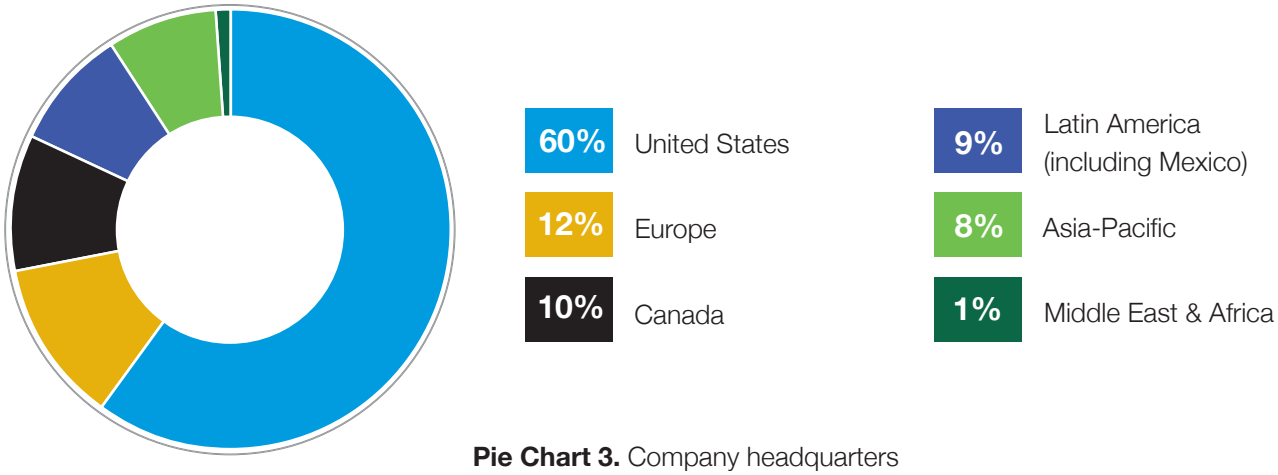
Pie Chart 1. Current position within the organization

As shown in Pie Chart 2, 23 percent of respondents report to the chief information officer, 21 percent report to the head of product engineering, 15 percent report to the head of DevOps, and 15 percent report to the chief information security officer.



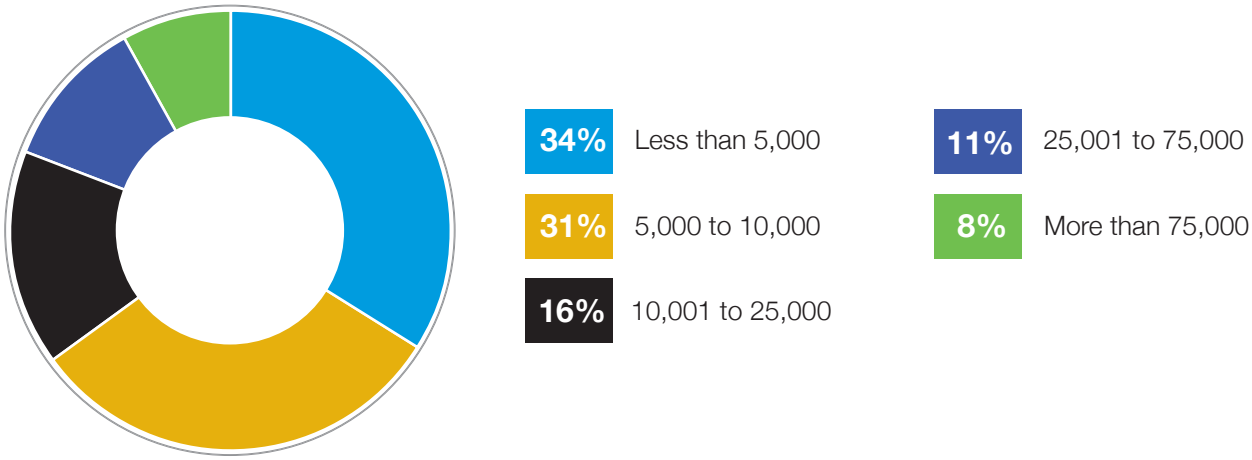
Pie Chart 2. Primary person you or your leader reports to

As shown in Pie Chart 3, the majority of respondents' organizations (60 percent) are headquartered in the United States. Another 12 percent have headquarters in Europe, and 10 percent are located in Canada.



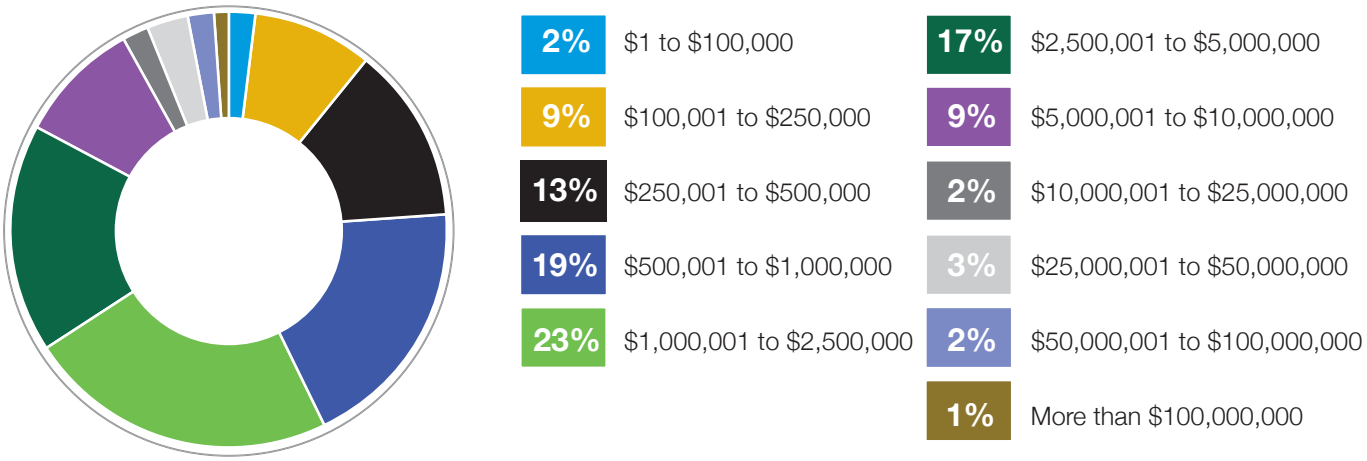
Pie Chart 3. Company headquarters

As shown in Pie Chart 4, 66 percent of respondents are from organizations with a global headcount of more than 5,000 employees.



Pie Chart 4. Worldwide headcount of the organization

When asked to choose the range that best approximates the total investment in terms of technologies, personnel, managed or outsourced services, and other cash outlays, 57 percent of respondents said their organizations are spending over $1 million, as shown in Pie Chart 5.



Pie Chart 5. Spending on automotive component security each year. Extrapolated value $6,098,000

Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of IT security practitioners and engineers in the automotive industry who are involved in contributing to or assessing the security of an automotive component. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from July 19, 2018 to August 3, 2018.

Sample response	**Freq.**	**Pct%**
• Total sample frame	15,900	100.0%
• Total returns	677	4.3%
• Rejected surveys	84	0.5%
• Final sample	593	3.7%

Part 1. Screening

S1a. Do you have any role or involvement in contributing to or assessing the security of an automotive component?	• Yes, significant involvement	32%
	• Yes, some involvement	50%
	• Yes, minimal involvement	18%
	• No involvement (Stop)	0%
	Total	100%

S1b. If you are involved, how many years have you spent contributing to or assessing the security of automotive devices?	• Less than 1 year	8%
	• 2 to 4 years	25%
	• 5 to 7 years	33%
	• 8 to 10 years	19%
	• More than 10 years	15%
	• Cannot determine (Stop)	0%
	Total	100%
	Extrapolated value	6.31

S2. What best describes your organization's role in development of automotive technology and/or components?	• Supplier	21%
	• Manufacturer	50%
	• Service provider	29%
	• None of the above (Stop)	0%
	Total	100%

Part 2. Background & organizational dynamics

Q1. What best describes your organization's position in the automotive industry?	• OEM	47%
	• Tier 1	36%
	• Tier 2	12%
	• Tier 3 or higher	3%
	• Other	2%
	Total	100%

Q2. Approximately, how many different types of automotive components or features are manufactured by your organization today?	• Less than 5	19%
	• 6 to 25	34%
	• 26 to 50	30%
	• More than 50	17%
	Total	100%
	Extrapolated value	27.63
Q3. What type of automotive software/technology/component does your organization design and develop? Please select all that apply.	• Infotainment systems	31%
	• Powertrain control units	37%
	• SOC system on chip-based components	17%
	• Self-driving (autonomous) vehicles	40%
	• Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)	30%
	• Telematics	49%
	• Steering systems	21%
	• Electrification components	36%
	• Cameras	28%
	• RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)	46%
	• Other (please specify)	2%
Q4. Which of the following best describes your organization's approach to product cybersecurity? Please select one choice only.	• Product cybersecurity is part of the traditional IT cybersecurity team (typically under a global CISO)	20%
	• Product cybersecurity is part of the functional safety team	17%
	• We have a centralized product cybersecurity team (i.e. center of excellence) that guides and supports multiple product development teams	10%
	• We have a decentralized product cybersecurity team, with cybersecurity experts attached to specific product development teams	23%
	• We do not have an established product cybersecurity program or team	30%
	Total	100%
Q5. How many FTEs participate in product cybersecurity management programs in your organization?	• Less than 5	30%
	• 5 to 10	44%
	• 11 to 20	18%
	• More than 20	8%
	Total	100%
	Extrapolated value	9.21
Q6. Does your organization allocate enough resources (i.e. budget and human resources) to cybersecurity?	• Yes	49%
	• No	51%
	Total	100%

Q7. Does your organization have the necessary cybersecurity skills in product development?	• Yes	38%
	• No	62%
	Total	100%

Q8. Do you feel empowered to raise concerns about the security of automotive technology in your organization?	• Yes	31%
	• No	69%
	Total	100%

Part 3. Perceptions about software security risk in the automotive industry

Q9. Which technologies pose the greatest cybersecurity risk? Please select all that apply.	• Infotainment systems	31%
	• Powertrain control units	46%
	• SOC system on chip-based components	44%
	• Self-driving (autonomous) vehicles	58%
	• Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)	51%
	• Telematics	60%
	• Steering systems	45%
	• Electrification components	17%
	• Cameras	29%
	• RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)	63%
	• Other (please specify)	2%

Q10. Are you aware of any of the following negative business impacts caused by insecure automotive software/technology/ components either developed or in use by your organization? Please select all that apply.	• Security-related recalls	21%
	• Damage to supply chain partner relationships	54%
	• Delayed or missed release dates	67%
	• Unintended interaction between components during integration testing	59%
	• Regulatory impacts, sanctions or fines	5%
	• Not aware of any adverse events	29%

Q11. Are you aware of any potential harm to drivers of vehicles because of insecure automotive software/technology/ components either developed or in use by your organization?	• Yes	52%
	• No	48%
	Total	100%

Q12. In your opinion, how likely is a malicious or proof-of-concept (i.e. security research) attack to occur against automotive software/technology/components developed or in use by your organization over the next 12 months?	• Very likely	27%
	• Likely	35%
	• Somewhat likely	23%
	• Not likely	15%
	Total	100%

Please rate the following statements using the 10-point scale from 1 = not concerned to 10 = very concerned.

Q13. How concerned are you about the cybersecurity posture of automotive software/technology/components developed by your organization?	• 1 or 2	13%
	• 3 or 4	12%
	• 5 or 6	23%
	• 7 or 8	26%
	• 9 or 10	26%
	Total	100%
	Extrapolated value	6.30

Q14. How concerned are you about the cybersecurity posture of automotive software/technology/components supplied to your organization by a third party?	• 1 or 2	8%
	• 3 or 4	4%
	• 5 or 6	15%
	• 7 or 8	30%
	• 9 or 10	43%
	Total	100%
	Extrapolated value	7.42

Q15. How concerned are you about the cybersecurity of the automotive industry as a whole?	• 1 or 2	9%
	• 3 or 4	6%
	• 5 or 6	17%
	• 7 or 8	28%
	• 9 or 10	40%
	Total	100%
	Extrapolated value	7.18

Q16. How concerned are you that your organization's cybersecurity practices are not keeping pace with changing automotive technologies?	• 1 or 2	5%
	• 3 or 4	11%
	• 5 or 6	25%
	• 7 or 8	22%
	• 9 or 10	37%
	Total	100%
	Extrapolated value	7.00

Q17. How concerned are you that regulatory cybersecurity requirements in the automotive industry are not keeping pace with changing automotive technologies?	• 1 or 2	12%
	• 3 or 4	16%
	• 5 or 6	29%
	• 7 or 8	23%
	• 9 or 10	20%
	Total	100%
	Extrapolated value	5.96
Q18. How concerned are you that regulatory cybersecurity requirements in the automotive industry are not very clear or well-defined?	• 1 or 2	10%
	• 3 or 4	19%
	• 5 or 6	27%
	• 7 or 8	25%
	• 9 or 10	19%
	Total	100%
	Extrapolated value	5.98
Q19. How concerned are you that a malicious actor may target the software/technology/components or vehicles produced by your organization?	• 1 or 2	15%
	• 3 or 4	7%
	• 5 or 6	10%
	• 7 or 8	33%
	• 9 or 10	35%
	Total	100%
	Extrapolated value	6.82
Q20. How confident are you that your organization can detect security vulnerabilities in automotive software/technology/components before going to market?	• 1 or 2	44%
	• 3 or 4	25%
	• 5 or 6	12%
	• 7 or 8	4%
	• 9 or 10	15%
	Total	100%
	Extrapolated value	3.92
Q21. How difficult is it for your organization to detect security vulnerabilities in automotive software/technology/components before going to market?	• 1 or 2	7%
	• 3 or 4	5%
	• 5 or 6	23%
	• 7 or 8	25%
	• 9 or 10	40%
	Total	100%
	Extrapolated value	7.22

Q22. How urgent is it for your organization to apply cybersecurity-related controls in automotive software/technology/components?	• 1 or 2	10%
	• 3 or 4	10%
	• 5 or 6	13%
	• 7 or 8	41%
	• 9 or 10	26%
	Total	100%
	Extrapolated value	6.76

Q23. Would any of the following factors influence your organization to increase the budget? Please select the top two factors.	• New regulations	35%
	• Vulnerability researcher disclosure	49%
	• A serious hacking incident of one of your automotive components	54%
	• Mandatory recall	60%
	• Other (please specify)	2%
	• None of the above	0%

Part 4. Security practices in the SDLC

Q24a. Does your organization provide secure development training for its software developers?	• Yes, it is optional	21%
	• Yes, it is mandatory	25%
	• Yes, only for certain teams	24%
	• No, we don't provide secure development training	30%
	Total	100%

Q24b. If yes, how effective is your organization's secure development training?	• Very effective	15%
	• Effective	21%
	• Somewhat effective	24%
	• Not effective	40%
	Total	100%

Q25. Does your organization follow an internally or externally published Secure Software Development Life Cycle (SSDLC) process for automotive software/technology/components?	• Yes, internally	35%
	• Yes, externally	29%
	• No	36%
	Total	100%

Q26. On average, what percentage of automotive software/technology/components developed or in use by your organization is tested for cybersecurity vulnerabilities?	None	25%
	Less than 25%	12%
	26% to 50%	26%
	51% to 75%	23%
	76% to 100%	14%
	Total	100%
	Extrapolated value	39%

Q27. When during the development life cycle does your organization assess automotive software/technology/components for security vulnerabilities? Please check all that apply.	• Requirements & design phase	19%
	• Development & testing phase	28%
	• Post release phase	43%
	• After integration into the vehicle network	37%
	• Post production release	18%

Q28. What activities does your organization employ to secure automotive software/technology/components? Please select all that apply.	• Educate developers on secure coding methods	33%
	• Secure architecture design	18%
	• Threat modeling	21%
	• Identification method	15%
	• Security requirements definitions	44%
	• Code review (manual)	29%
	• Static analysis/SAST (automated)	47%
	• System debugging	48%
	• Fuzz testing	19%
	• Software composition analysis	18%
	• Dynamic security testing/DAST	49%
	• Penetration testing	56%
	• Data masking or redaction of live data (during testing)	39%
	• Security patch management	61%
	• Run-time application self-protection	26%
	• Other (please specify)	3%
	• None of the above	8%

Q29. Does your organization use open source code in the automotive software/technology/components developed by your organization?	• Yes, we have an established process for inventorying and managing open source code in use	26%
	• Yes, we use open source code but do not have an established process for inventorying and managing its use	32%
	• No, we do not use open source code	42%
	Total	100%

Q30. What are the primary factors that lead to vulnerabilities in the automotive software/technology/components developed or in use by your organization. Please select the top four factors.	• Accidental coding errors	55%
	• The use of insecure/outdated open source software components	40%
	• Malicious code injection	23%
	• Lack of internal policies or rules that clarify security requirements	26%
	• Lack of understanding/training on secure coding practices	60%
	• Pressure to meet product deadlines	71%
	• Lack of quality assurance and testing procedures	50%
	• Product development tools have inherent bugs	39%
	• Incorrect permissions	19%
	• Back end systems	15%
	• Other (please specify)	2%

Q31. Do you have an incident response plan in place in the event of a critical vulnerability disclosure?	• Yes	43%
	• No	57%
	Total	100%
Q32. Does your organization incorporate any security counter measures in its vehicles? Please check all that apply.	• Gateways	59%
	• Firewalls	64%
	• Machine learning	41%
	• Whitelisting	38%
	• Other (please specify)	3%
Q33a. Does your organization use key management systems for software/technology/components used in the development or manufacturing process?	Yes	63%
	No	37%
	Total	100%
Q33b. If yes, what key management systems does your organization presently use? Please check all that apply.	• Formal Key Management Policy (KMP)	45%
	• Manual process (e.g. spreadsheet, paper-based)	43%
	• Central key management system/server	56%
	• Hardware security modules	39%
	• Other	2%
Q34. How does your organization deliver security patches and updates for vehicles in-market?	• Over the Air (OTA) updates	37%
	• Aftermarket maintenance	45%
	• Through wireless communications connected to personal electronic/computing devices	51%
	• Through procured software, components and systems	65%
	• We don't deliver security updates	25%
	• Other	3%
Q35. If you don't deliver OTA updates, do you plan to in the future?	• Yes, in 1 to 3 years	33%
	• Yes, in 3 to 5 years	23%
	• Greater than 5 years	9%
	• No plans to deliver OTA updates	35%
	Total	100%
Q36. Does your organization's software update delivery model address critical security vulnerabilities in a timely manner?	• Yes	39%
	• No	61%
	Total	100%

Part 5. Cybersecurity supply chain practices

Q37a. Does your organization impose cybersecurity requirements for automotive software/technology/components provided by upstream suppliers?	Yes	44%
	No (skip to Q38)	56%
	Total	100%
Q37b. If yes, how does your organization ensure that suppliers adhere to security requirements? Please check all that apply.	• Suppliers are required to self-assess and provide verification and validation	51%
	• A third party is required to assess and provide independent verification and validation	25%
	• We perform supplier security assessments directly	38%
	• Security requirements are explicitly defined in supplier agreements	49%
	• We do not have a formal process for ensuring suppliers' adherence to security requirements (skip to Q38)	40%
Q37c. If yes, how often does your organization require security assurance from suppliers?	• Annually	33%
	• Quarterly	9%
	• For every major release	26%
	• Every time the code changes	29%
	• Other	3%
	Total	100%

Part 6. Future automotive industry practices

Q38. What future network architectures will enhance vehicle security?	• Automotive Ethernet	44%
	• FlexRay	50%
	• 5g	54%
	• Other (please explain)	8%
	• None of the above	26%
Q39. What targeted standards/ guidelines/technologies will create a more secure/resilient vehicle network?	• Security module	29%
	• Gateways	50%
	• IDS	54%
	• Secure OTA update	63%
	• Whitelisting	47%
	• Other (please explain)	5%

Q40. What is the most effective and attainable security assurance testing/certification/accreditation approach?	• Self-certification	20%
	• Self-certification in compliance with a process standard	40%
	• Self-certification with periodic assessments	32%
	• Type certification	8%
	• Other (please explain)	0%
	Total	100%

Part 7. Demographics & organizational characteristics

D1. What organizational level best describes your current position?	• Senior Executive/VP	3%
	• Director	12%
	• Manager	19%
	• Supervisor	11%
	• Engineer	15%
	• Technician	21%
	• Staff	13%
	• Contractor	3%
	• Other	3%
	Total	100%

D2. Check the Primary Person you or your leader reports to within the organization.	• Chief Financial Officer	0%
	• Chief Operations Officer	0%
	• General Counsel	2%
	• Head, DevOps	15%
	• Head, Product Engineering	21%
	• Head, Quality Assurances	7%
	• Chief Information Officer	23%
	• Chief Technology Officer	9%
	• Chief Information Security Officer	15%
	• Chief Security Officer	0%
	• Compliance Officer	3%
	• Data Center Management	2%
	• Chief Risk Officer	3%
	• Other	0%
	Total	100%

D3. Where is your company headquartered?	• United States	60%
	• Canada	10%
	• Europe	12%
	• Middle East & Africa	1%
	• Asia-Pacific	8%
	• Latin America (including Mexico)	9%
	Total	100%

D4. What is the worldwide headcount of your company?	• Less than 5,000	34%
	• 5,000 to 10,000	31%
	• 10,001 to 25,000	16%
	• 25,001 to 75,000	11%
	• More than 75,000	8%
	Total	100%

D5. Approximately, how much does your organization spend on automotive component security each year? Please choose the range that best approximates the total investment in terms of technologies, personnel, managed or outsourced services and other cash outlays.	• None	0%
	• $1 to $100,000	2%
	• $100,001 to $250,000	9%
	• $250,001 to $500,000	13%
	• $500,001 to $1,000,000	19%
	• $1,000,001 to $2,500,000	23%
	• $2,500,001 to $5,000,000	17%
	• $5,000,001 to $10,000,000	9%
	• $10,000,001 to $25,000,000	2%
	• $25,000,001 to $50,000,000	3%
	• $50,000,001 to $100,000,000	2%
	• More than $100,000,000	1%
	Total	100%
	Extrapolated value (US$)	$6,098,000

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.