Securing the Modern Vehicle:
A Study of Automotive Industry Cybersecurity Practices

An independent study commissioned by

Ponemon Institute

SAE International

Synopsys®
Table of Contents

Executive Summary .......................................................................................................................... 1
Organizational Dynamics and Challenges ....................................................................................... 3
Technical Dynamics and Challenges ............................................................................................... 6
Product Development and Security Testing Practices ................................................................. 9
Supply Chain and Third-Party Component Challenges ............................................................. 13
Conclusions .................................................................................................................................. 14
Methods ...................................................................................................................................... 15
Appendix: Detailed Survey Results .............................................................................................. 18
Ponemon Institute ......................................................................................................................... 29
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.

- 84% have concerns that cybersecurity practices are not keeping pace with evolving technologies
- 30% do not have an established product cybersecurity program or team
- 63% 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](image)

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

| Are you aware of potential harms to drivers? | 52% |
| Do you feel empowered to raise concerns?    | 31% |

<table>
<thead>
<tr>
<th>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?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
</tr>
<tr>
<td>Likely</td>
</tr>
<tr>
<td>Somewhat likely</td>
</tr>
<tr>
<td>Not likely</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Do you feel empowered to raise concerns about the security of automotive technology in your organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>
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.

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? 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%
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.

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

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>5%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>11%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>25%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>22%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>37%</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infotainment systems</td>
<td>31%</td>
</tr>
<tr>
<td>Powertrain control units</td>
<td>46%</td>
</tr>
<tr>
<td>SOC system on chip-based components</td>
<td>44%</td>
</tr>
<tr>
<td><strong>Self-driving (autonomous) vehicles</strong></td>
<td>58%</td>
</tr>
<tr>
<td>Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)</td>
<td>51%</td>
</tr>
<tr>
<td><strong>Telematics</strong></td>
<td>60%</td>
</tr>
<tr>
<td>Steering systems</td>
<td>45%</td>
</tr>
<tr>
<td>Electrification components</td>
<td>17%</td>
</tr>
<tr>
<td>Cameras</td>
<td>29%</td>
</tr>
<tr>
<td>RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)</td>
<td>63%</td>
</tr>
</tbody>
</table>
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.

![Bar Chart](chart.png)

**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.

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.
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?](image)

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.

---

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.

<table>
<thead>
<tr>
<th>What percentage of automotive technology used by your organization is tested for cybersecurity vulnerabilities?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• None                                                       25%</td>
</tr>
<tr>
<td>• Less than 25%                                               12%</td>
</tr>
<tr>
<td>• 26% to 50%                                                  26%</td>
</tr>
<tr>
<td>• 51% to 75%                                                  23%</td>
</tr>
<tr>
<td>• 76% to 100%                                                 14%</td>
</tr>
<tr>
<td>Total                                                        100%</td>
</tr>
</tbody>
</table>

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?

- **Pressure to meet product deadlines** 71%
- **Lack of understanding/training on secure coding practices** 60%
- **Accidental coding errors** 55%
- **Lack of quality assurance and testing procedures** 50%
- **The use of insecure/outdated open source software components** 40%
- **Product development tools have inherent bugs** 39%
- **Lack of internal policies or rules that clarify security requirements** 26%
- **Malicious code injection** 23%
- **Incorrect permissions** 19%
- **Back end systems** 15%
- **Other** 2%
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.

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>
<thead>
<tr>
<th>Table 1. Sample response</th>
<th>Freq.</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Total sample frame</td>
<td>15,900</td>
<td>100.0%</td>
</tr>
<tr>
<td>• Total returns</td>
<td>677</td>
<td>4.3%</td>
</tr>
<tr>
<td>• Rejected surveys</td>
<td>84</td>
<td>0.5%</td>
</tr>
<tr>
<td>• Final sample</td>
<td>593</td>
<td>3.7%</td>
</tr>
</tbody>
</table>

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

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.
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.

<table>
<thead>
<tr>
<th>Sample response</th>
<th>Freq.</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Total sample frame</td>
<td>15,900</td>
<td>100.0%</td>
</tr>
<tr>
<td>• Total returns</td>
<td>677</td>
<td>4.3%</td>
</tr>
<tr>
<td>• Rejected surveys</td>
<td>84</td>
<td>0.5%</td>
</tr>
<tr>
<td>• Final sample</td>
<td>593</td>
<td>3.7%</td>
</tr>
</tbody>
</table>

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?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 5</td>
<td>19%</td>
</tr>
<tr>
<td>6 to 25</td>
<td>34%</td>
</tr>
<tr>
<td>26 to 50</td>
<td>30%</td>
</tr>
<tr>
<td>More than 50</td>
<td>17%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Extrapolated value: 27.63

### Q3. What type of automotive software/technology/component does your organization design and develop? Please select all that apply.

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infotainment systems</td>
<td>31%</td>
</tr>
<tr>
<td>Powertrain control units</td>
<td>37%</td>
</tr>
<tr>
<td>SOC system on chip-based components</td>
<td>17%</td>
</tr>
<tr>
<td>Self-driving (autonomous) vehicles</td>
<td>40%</td>
</tr>
<tr>
<td>Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)</td>
<td>30%</td>
</tr>
<tr>
<td>Telematics</td>
<td>49%</td>
</tr>
<tr>
<td>Steering systems</td>
<td>21%</td>
</tr>
<tr>
<td>Electrification components</td>
<td>36%</td>
</tr>
<tr>
<td>Cameras</td>
<td>28%</td>
</tr>
<tr>
<td>RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)</td>
<td>46%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
</tbody>
</table>

### Q4. Which of the following best describes your organization’s approach to product cybersecurity? Please select one choice only.

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product cybersecurity is part of the traditional IT cybersecurity team (typically under a global CISO)</td>
<td>20%</td>
</tr>
<tr>
<td>Product cybersecurity is part of the functional safety team</td>
<td>17%</td>
</tr>
<tr>
<td>We have a centralized product cybersecurity team (i.e. center of excellence) that guides and supports multiple product development teams</td>
<td>10%</td>
</tr>
<tr>
<td>We have a decentralized product cybersecurity team, with cybersecurity experts attached to specific product development teams</td>
<td>23%</td>
</tr>
<tr>
<td>We do not have an established product cybersecurity program or team</td>
<td>30%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### Q5. How many FTEs participate in product cybersecurity management programs in your organization?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 5</td>
<td>30%</td>
</tr>
<tr>
<td>5 to 10</td>
<td>44%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>18%</td>
</tr>
<tr>
<td>More than 20</td>
<td>8%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Extrapolated value: 9.21

### Q6. Does your organization allocate enough resources (i.e. budget and human resources) to cybersecurity?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>49%</td>
</tr>
<tr>
<td>No</td>
<td>51%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
Q7. Does your organization have the necessary cybersecurity skills in product development?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>38%</td>
<td>62%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
</tr>
</tbody>
</table>

Q8. Do you feel empowered to raise concerns about the security of automotive technology in your organization?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>31%</td>
<td>69%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
</tr>
</tbody>
</table>

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

Q9. Which technologies pose the greatest cybersecurity risk? Please select all that apply.

<table>
<thead>
<tr>
<th>Technologies</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infotainment systems</td>
<td>31%</td>
</tr>
<tr>
<td>Powertrain control units</td>
<td>46%</td>
</tr>
<tr>
<td>SOC system on chip-based components</td>
<td>44%</td>
</tr>
<tr>
<td>Self-driving (autonomous) vehicles</td>
<td>58%</td>
</tr>
<tr>
<td>Software-focused service provider (e.g. cloud, insurance provider, streaming service, etc.)</td>
<td>51%</td>
</tr>
<tr>
<td>Telematics</td>
<td>60%</td>
</tr>
<tr>
<td>Steering systems</td>
<td>45%</td>
</tr>
<tr>
<td>Electrification components</td>
<td>17%</td>
</tr>
<tr>
<td>Cameras</td>
<td>29%</td>
</tr>
<tr>
<td>RF technologies (e.g. Wi-Fi, Bluetooth, Hot spots)</td>
<td>63%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Negative business impacts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security-related recalls</td>
<td>21%</td>
</tr>
<tr>
<td>Damage to supply chain partner relationships</td>
<td>54%</td>
</tr>
<tr>
<td>Delayed or missed release dates</td>
<td>67%</td>
</tr>
<tr>
<td>Unintended interaction between components during integration testing</td>
<td>59%</td>
</tr>
<tr>
<td>Regulatory impacts, sanctions or fines</td>
<td>5%</td>
</tr>
<tr>
<td>Not aware of any adverse events</td>
<td>29%</td>
</tr>
</tbody>
</table>

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?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>52%</td>
<td>48%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
</tr>
</tbody>
</table>
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 |

<p>| 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 |</p>
<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q17. How concerned are you that regulatory cybersecurity requirements in the automotive industry are not keeping pace with changing automotive technologies?</td>
<td>1 or 2</td>
<td>12%</td>
</tr>
<tr>
<td></td>
<td>3 or 4</td>
<td>16%</td>
</tr>
<tr>
<td></td>
<td>5 or 6</td>
<td>29%</td>
</tr>
<tr>
<td></td>
<td>7 or 8</td>
<td>23%</td>
</tr>
<tr>
<td></td>
<td>9 or 10</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>Extrapolated value 5.96</td>
</tr>
<tr>
<td>Q18. How concerned are you that regulatory cybersecurity requirements in the automotive industry are not very clear or well-defined?</td>
<td>1 or 2</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>3 or 4</td>
<td>19%</td>
</tr>
<tr>
<td></td>
<td>5 or 6</td>
<td>27%</td>
</tr>
<tr>
<td></td>
<td>7 or 8</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>9 or 10</td>
<td>19%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>Extrapolated value 5.98</td>
</tr>
<tr>
<td>Q19. How concerned are you that a malicious actor may target the software/technology/components or vehicles produced by your organization?</td>
<td>1 or 2</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>3 or 4</td>
<td>7%</td>
</tr>
<tr>
<td></td>
<td>5 or 6</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>7 or 8</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>9 or 10</td>
<td>35%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>Extrapolated value 6.82</td>
</tr>
<tr>
<td>Q20. How confident are you that your organization can detect security vulnerabilities in automotive software/technology/components before going to market?</td>
<td>1 or 2</td>
<td>44%</td>
</tr>
<tr>
<td></td>
<td>3 or 4</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>5 or 6</td>
<td>12%</td>
</tr>
<tr>
<td></td>
<td>7 or 8</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>9 or 10</td>
<td>15%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>Extrapolated value 3.92</td>
</tr>
<tr>
<td>Q21. How difficult is it for your organization to detect security vulnerabilities in automotive software/technology/components before going to market?</td>
<td>1 or 2</td>
<td>7%</td>
</tr>
<tr>
<td></td>
<td>3 or 4</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>5 or 6</td>
<td>23%</td>
</tr>
<tr>
<td></td>
<td>7 or 8</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>9 or 10</td>
<td>40%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>Extrapolated value 7.22</td>
</tr>
</tbody>
</table>
Q22. How urgent is it for your organization to apply cybersecurity-related controls in automotive software/technology/components?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>10%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>10%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>13%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>41%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>26%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Extrapolated value</td>
<td>6.76</td>
</tr>
</tbody>
</table>

Q23. Would any of the following factors influence your organization to increase the budget? Please select the top two factors.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>New regulations</td>
<td>35%</td>
</tr>
<tr>
<td>Vulnerability researcher disclosure</td>
<td>49%</td>
</tr>
<tr>
<td>A serious hacking incident of one of your automotive components</td>
<td>54%</td>
</tr>
<tr>
<td>Mandatory recall</td>
<td>60%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
<tr>
<td>None of the above</td>
<td>0%</td>
</tr>
</tbody>
</table>

Part 4. Security practices in the SDLC

Q24a. Does your organization provide secure development training for its software developers?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, it is optional</td>
<td>21%</td>
</tr>
<tr>
<td>Yes, it is mandatory</td>
<td>25%</td>
</tr>
<tr>
<td>Yes, only for certain teams</td>
<td>24%</td>
</tr>
<tr>
<td>No, we don’t provide secure development training</td>
<td>30%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q24b. If yes, how effective is your organization’s secure development training?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very effective</td>
<td>15%</td>
</tr>
<tr>
<td>Effective</td>
<td>21%</td>
</tr>
<tr>
<td>Somewhat effective</td>
<td>24%</td>
</tr>
<tr>
<td>Not effective</td>
<td>40%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q25. Does your organization follow an internally or externally published Secure Software Development Life Cycle (SSDLC) process for automotive software/technology/components?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, internally</td>
<td>35%</td>
</tr>
<tr>
<td>Yes, externally</td>
<td>29%</td>
</tr>
<tr>
<td>No</td>
<td>36%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q26. On average, what percentage of automotive software/technology/components developed or in use by your organization is tested for cybersecurity vulnerabilities?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>25%</td>
</tr>
<tr>
<td>Less than 25%</td>
<td>12%</td>
</tr>
<tr>
<td>26% to 50%</td>
<td>26%</td>
</tr>
<tr>
<td>51% to 75%</td>
<td>23%</td>
</tr>
<tr>
<td>76% to 100%</td>
<td>14%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Extrapolated value</td>
<td>39%</td>
</tr>
</tbody>
</table>
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 26%
- 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/obtained 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%
<table>
<thead>
<tr>
<th>Question</th>
<th>Response Options</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q31. Do you have an incident response plan in place in the event of a critical vulnerability disclosure?</td>
<td>• Yes</td>
<td>43%</td>
</tr>
<tr>
<td></td>
<td>• No</td>
<td>57%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Q32. Does your organization incorporate any security counter measures in its vehicles? Please check all that apply.</td>
<td>• Gateways</td>
<td>59%</td>
</tr>
<tr>
<td></td>
<td>• Firewalls</td>
<td>64%</td>
</tr>
<tr>
<td></td>
<td>• Machine learning</td>
<td>41%</td>
</tr>
<tr>
<td></td>
<td>• Whitelisting</td>
<td>38%</td>
</tr>
<tr>
<td></td>
<td>• Other (please specify)</td>
<td>3%</td>
</tr>
<tr>
<td>Q33a. Does your organization use key management systems for software/technology/components used in the development or manufacturing process?</td>
<td>Yes</td>
<td>63%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>37%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Q33b. If yes, what key management systems does your organization presently use? Please check all that apply.</td>
<td>• Formal Key Management Policy (KMP)</td>
<td>45%</td>
</tr>
<tr>
<td></td>
<td>• Manual process (e.g. spreadsheet, paper-based)</td>
<td>43%</td>
</tr>
<tr>
<td></td>
<td>• Central key management system/server</td>
<td>56%</td>
</tr>
<tr>
<td></td>
<td>• Hardware security modules</td>
<td>39%</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
<td>2%</td>
</tr>
<tr>
<td>Q34. How does your organization deliver security patches and updates for vehicles in-market?</td>
<td>• Over the Air (OTA) updates</td>
<td>37%</td>
</tr>
<tr>
<td></td>
<td>• Aftermarket maintenance</td>
<td>45%</td>
</tr>
<tr>
<td></td>
<td>• Through wireless communications connected to personal electronic/computing devices</td>
<td>51%</td>
</tr>
<tr>
<td></td>
<td>• We don’t deliver security updates</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
<td>3%</td>
</tr>
<tr>
<td>Q35. If you don’t deliver OTA updates, do you plan to in the future?</td>
<td>• Yes, in 1 to 3 years</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>• Yes, in 3 to 5 years</td>
<td>23%</td>
</tr>
<tr>
<td></td>
<td>• Greater than 5 years</td>
<td>9%</td>
</tr>
<tr>
<td></td>
<td>• No plans to deliver OTA updates</td>
<td>35%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Q36. Does your organization’s software update delivery model address critical security vulnerabilities in a timely manner?</td>
<td>• Yes</td>
<td>39%</td>
</tr>
<tr>
<td></td>
<td>• No</td>
<td>61%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Part 5. Cybersecurity supply chain practices

Q37a. Does your organization impose cybersecurity requirements for automotive software/technology/components provided by upstream suppliers?

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>44%</td>
</tr>
<tr>
<td>No (skip to Q38)</td>
<td>56%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q37b. If yes, how does your organization ensure that suppliers adhere to security requirements? Please check all that apply.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppliers are required to self-assess and provide verification and validation</td>
<td>51%</td>
</tr>
<tr>
<td>A third party is required to assess and provide independent verification and validation</td>
<td>25%</td>
</tr>
<tr>
<td>We perform supplier security assessments directly</td>
<td>38%</td>
</tr>
<tr>
<td>Security requirements are explicitly defined in supplier agreements</td>
<td>49%</td>
</tr>
<tr>
<td>We do not have a formal process for ensuring suppliers’ adherence to security requirements (skip to Q38)</td>
<td>40%</td>
</tr>
</tbody>
</table>

Q37c. If yes, how often does your organization require security assurance from suppliers?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annually</td>
<td>33%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>9%</td>
</tr>
<tr>
<td>For every major release</td>
<td>26%</td>
</tr>
<tr>
<td>Every time the code changes</td>
<td>29%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Part 6. Future automotive industry practices

Q38. What future network architectures will enhance vehicle security?

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive Ethernet</td>
<td>44%</td>
</tr>
<tr>
<td>FlexRay</td>
<td>50%</td>
</tr>
<tr>
<td>5g</td>
<td>54%</td>
</tr>
<tr>
<td>Other (please explain)</td>
<td>8%</td>
</tr>
<tr>
<td>None of the above</td>
<td>26%</td>
</tr>
</tbody>
</table>

Q39. What targeted standards/guidelines/technologies will create a more secure/resilient vehicle network?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security module</td>
<td>29%</td>
</tr>
<tr>
<td>Gateways</td>
<td>50%</td>
</tr>
<tr>
<td>IDS</td>
<td>54%</td>
</tr>
<tr>
<td>Secure OTA update</td>
<td>63%</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>47%</td>
</tr>
<tr>
<td>Other (please explain)</td>
<td>5%</td>
</tr>
</tbody>
</table>
### 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?

<table>
<thead>
<tr>
<th>Position</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Executive/VP</td>
<td>3%</td>
</tr>
<tr>
<td>Director</td>
<td>12%</td>
</tr>
<tr>
<td>Manager</td>
<td>19%</td>
</tr>
<tr>
<td>Supervisor</td>
<td>11%</td>
</tr>
<tr>
<td>Engineer</td>
<td>15%</td>
</tr>
<tr>
<td>Technician</td>
<td>21%</td>
</tr>
<tr>
<td>Staff</td>
<td>13%</td>
</tr>
<tr>
<td>Contractor</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Total** 100%

#### D2. Check the Primary Person you or your leader reports to within the organization.

<table>
<thead>
<tr>
<th>Position</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Financial Officer</td>
<td>0%</td>
</tr>
<tr>
<td>Chief Operations Officer</td>
<td>0%</td>
</tr>
<tr>
<td>General Counsel</td>
<td>2%</td>
</tr>
<tr>
<td>Head, DevOps</td>
<td>15%</td>
</tr>
<tr>
<td>Head, Product Engineering</td>
<td>21%</td>
</tr>
<tr>
<td>Head, Quality Assurances</td>
<td>7%</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>23%</td>
</tr>
<tr>
<td>Chief Technology Officer</td>
<td>9%</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>15%</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>0%</td>
</tr>
<tr>
<td>Compliance Officer</td>
<td>3%</td>
</tr>
<tr>
<td>Data Center Management</td>
<td>2%</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Total** 100%

#### D3. Where is your company headquartered?

<table>
<thead>
<tr>
<th>Location</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>60%</td>
</tr>
<tr>
<td>Canada</td>
<td>10%</td>
</tr>
<tr>
<td>Europe</td>
<td>12%</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>1%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>8%</td>
</tr>
<tr>
<td>Latin America (including Mexico)</td>
<td>9%</td>
</tr>
</tbody>
</table>

**Total** 100%
### D4. What is the worldwide headcount of your company?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 5,000</td>
<td>34%</td>
</tr>
<tr>
<td>5,000 to 10,000</td>
<td>31%</td>
</tr>
<tr>
<td>10,001 to 25,000</td>
<td>16%</td>
</tr>
<tr>
<td>25,001 to 75,000</td>
<td>11%</td>
</tr>
<tr>
<td>More than 75,000</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0%</td>
</tr>
<tr>
<td>$1 to $100,000</td>
<td>2%</td>
</tr>
<tr>
<td>$100,001 to $250,000</td>
<td>9%</td>
</tr>
<tr>
<td>$250,001 to $500,000</td>
<td>13%</td>
</tr>
<tr>
<td>$500,001 to $1,000,000</td>
<td>19%</td>
</tr>
<tr>
<td>$1,000,001 to $2,500,000</td>
<td>23%</td>
</tr>
<tr>
<td>$2,500,001 to $5,000,000</td>
<td>17%</td>
</tr>
<tr>
<td>$5,000,001 to $10,000,000</td>
<td>9%</td>
</tr>
<tr>
<td>$10,000,001 to $25,000,000</td>
<td>2%</td>
</tr>
<tr>
<td>$25,000,001 to $50,000,000</td>
<td>3%</td>
</tr>
<tr>
<td>$50,000,001 to $100,000,000</td>
<td>2%</td>
</tr>
<tr>
<td>More than $100,000,000</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

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.

© 2018 Synopsys, Inc. and SAE International