https://deloitte.wsj.com/articles/how-to-help-secure-automotive-software-01666620593

TECHNOLOGY | CONSUMER PRODUCTS | CYBERSECURITY

How to Help Secure Automotive Software

Vehicles are becoming more connected and reliant on software and data, but the road ahead still may be bumpy

A focus on communication and collaboration appears central to effectively implementing cybersecurity standards related to autonomous vehicles (AVs) and electric vehicles (EVs)—a focus that offers much-anticipated guidance to an industry navigating a segmented and still evolving regulatory landscape.

The international standard, ISO/SAE 21434, which was released about a year ago, provides leading practices to address automotive cybersecurity. Its goal is to promote cybersecurity for all road vehicles and their electronic systems and to encourage original equipment manufacturers (OEMs) and Tier 1 suppliers to consider cybersecurity at every step of their product development life cycle, from the concept phase to product retirement.

“There was limited direction and guidance in place prior to ISO/SAE 21434, yet automotive customers expect the industry to actively address cybersecurity challenges in a consistent way,” says Leon Nash, a principal with Deloitte Risk & Financial Advisory, Deloitte & Touche LLP. “Many OEMs and Tier 1 suppliers were looking for well-crafted industry standards that could provide clear direction, and this guidance should deliver some anticipated clarity.”

The standard introduces a threat agent risk assessment, which helps identify, assess, prioritize, and control cybersecurity risks to determine critical exposures while also considering mitigation controls and accepted levels of risk. Further, ISO/SAE 21434 addresses cybersecurity governance and organizational structure and spells out key processes that OEMs and suppliers can build across the product development life cycle. It encourages companies to move away from waterfall development to a more agile approach where the basics of cybersecurity controls, activities, processes, and frameworks are incorporated earlier in the engineering process.

“As software becomes an inherent and substantial part of today’s AV/EV, software-based risks are more critical than risks from other components,” says Nishant Khadria, a risk advisory director at Deloitte Germany. “The adverse impacts of software defects in a connected ecosystem of software-defined vehicles (SDV) could be massive, which makes it indispensable to practicing security and privacy by design.”

This standard also helps implementing a cybersecurity management system as required by United Nations Economic Commission for Europe (UNECE) R155v. “Many automotive companies across the globe have adopted ISO/SAE 21434 as a benchmark for their engineering processes including threat analysis and risk assessment,” adds Khadria.

Communicate, Collaborate

In addition to introducing threat analysis and risk assessments early in the product development process, there are several other leading practices OEMs can deploy to secure software, which requires clear communication and genuine collaboration between the C-suite, board, information security team, and third-party suppliers.

Indeed, the spectrum of risks that can emanate from a cyberattack is broad, ranging from business disruption to negative brand and reputation impacts. Nash notes that one of the biggest risks organizations face often stems from third-party cyber risk, which can be pervasive in the automotive industry where corporations do business with or have services provided by a multitude of third parties. Those entities can range from IT and SaaS solutions providers to outsourced sales and marketing support and third-party companies that build a portion of a digital product. Suppliers also work with thousands of third parties creating the potential for a broad attack surface.

Having visibility into third parties’ security controls and being able to manage and dictate how third parties behave when they’re handling another organization’s data can allow an original equipment manufacturer (OEM) to prevent a potential attack and the ensuing loss of data, reputational damage, and hefty fines. “Corporations can use periodic checks, via surveys, in addition to annual assessments to gauge whether a third-party supplier’s risk profile was affected by business or technology transformation activities, such as a move to the cloud,” recommends Nash.

In addition to gathering information from third parties to understand the way they collect and protect data, organizations should also have clear and solid communication channels with all parties to define cybersecurity interfaces and requirements and to manage and patch software vulnerabilities.

In turn, it’s important for the C-suite, board, and audit committee to understand the potential risks, weigh them against the organization’s risk appetite, and set up mechanisms to stay informed about progress related to the build-out of cybersecurity capabilities, services, controls, and frameworks. A focus on communication can also help leaders determine an appropriate cybersecurity budget in a timely fashion.

“When it comes to reporting on cybersecurity risk and communicating the value of cybersecurity controls and investments, security leaders should use a language that resonates with the board members and the C-suite” says Shima Mousavi, a senior manager with Deloitte Risk & Financial Advisory, Deloitte & Touche LLP. “Companies want to make sure that the chief information security officer (CISO) or business information security officer (BISO) can get the value of cybersecurity across and can articulate the risk and impact on the business without being too technical.”

Effective CISOs and BISOs also can help frame cyber risk, encouraging the C-suite and board to view cyber risk as more than just an IT or information security risk, but rather a business risk. To promote that kind of communication and collaboration, the automotive industry may need to rethink their employee skill sets.

“Modern product development teams should be comprised of professionals with a mix of software development experience, automotive, and cybersecurity knowledge” says Mousavi. “Product professionals with a background in threat analysis, vulnerability management, and an understanding of the software development life cycle are highly in demand, particularly as new standards such as ISO/SAE 21434 are being implemented. But finding that mix can be a challenge.”

Road Ahead Likely Requires More Collaboration

Addressing cybersecurity in the evolving automotive industry may not always be smooth, but communication and collaboration can help. Consider where security related to AVs and EVs is paramount: data, software, and connectivity. These vehicles are using AI and machine learning algorithms, which are heavily reliant on high quality data. As data loads increase, it is critical that OEMs pay greater attention to securing and protecting this data from a privacy and security perspective.

OEMs are adopting software-defined vehicle architectures that enable them to tap into cloud-based revenue streams and provide customers with additional safety and connectivity features. “As a result, there is an increased need for software security, especially as OEMs shift to open-source software models to reduce development time and added investment,” notes Mousavi.

In addition, as OEMs open their doors to more suppliers and connected devices, connectivity and information sharing across the industry are on the rise, and security on that front is also becoming a greater need. With the advent and deployment of 5G, more data is flowing not only between mobile devices and vehicles, but also to the cloud and other third parties that may be involved in the development and manufacturing processes, increasing the overall cyberattack surface.

OEMs and suppliers are also addressing a fragmented and developing regulatory environment. The National Institute of Standards and Technology has been working with different OEMs to promote physical security, cybersecurity standards, and leading practices across all data mediums. Concurrently, the UNECE has mandated new regulations for cybersecurity management systems for new vehicles that are being produced for the European market. The ISO/SAE 21434 outlines process requirements for cybersecurity risk management and product development of road vehicle systems, including the complete life cycle from concept, development, production, operations and maintenance, to decommissioning. ISO/SAE 21434 is a tactical means to achieve the goal of complying with UNECE.

“The current regulatory environment is evolving and, although it’s not quite where it needs to be, it’s generally heading in the right direction,” says Nash, adding that one of the reasons for this fragmentation is the decentralized establishment of regulations and standards across global regions.

Although most OEMs function and operate on a global level, regulations vary from market to market, including in the United States, where data privacy regulations are being generated at the state level and can differ from one state to another. This distributed nature presents a challenge as OEMs trying to comply with different regulations may need to assess the same controls multiple times, which introduce inefficiencies and unnecessary resource allocation.

The regulatory framework is also segmented. Nash explains that while UNECE covers cybersecurity management systems and software update management, those two areas are treated separately. Meanwhile, other tangential areas such as data privacy and consumer protection are regulated by a separate set of standards that aren't tied together.

By enhancing their approach to communication and collaboration, organizations can elevate cybersecurity to the appropriate level, ultimately allowing the automotive industry to address and mitigate cybersecurity-related challenges and focus on other tasks such as going to market and improving customer experience.

"The challenge for many organizations is to effectively implement new cybersecurity standards and validate that they've met the spirit of regulations and standards. That's where the rubber hits the road," Nash says.

"Implementing new standards always comes at a cost; however, through secure software development process and better collaboration between internal and external stakeholders, cybersecurity can be efficiently achieved," adds Nishant.

—Marine Cole, senior writer, Deloitte Services LP, Deloitte Insights in The Wall Street Journal

PUBLISHED ON: Oct. 24, 2022 3:00 pm ET

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United

MORE DELOITTE INSIGHTS ARTICLES

A New Approach to Resilience

Metaverse and Web3: The Next Internet Platform

Government Customer Experience Could Hold the Key to Citizens' Trust

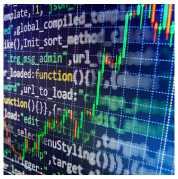
The Future of Cloud: 7 Lessons From Leaders

SEARCH DELOITTE ARTICLES

WHAT'S TRENDING

1. **Board Agenda: Cyber in an Era of Escalating Risk and Regulatory Focus**

2. **Rethink Responses to Cyber Risks in Financial Services**



3. **At Bank of America, Data Advances DEI**

ABOUT DELOITTE INSIGHTS

Deloitte's Insights for C-suite executives and board members provide information and resources to help address the challenges of managing risk for both value creation and protection, as well as increasing compliance requirements.

For relevant content at your fingertips, download the Deloitte Insights app.