Deloitte.
Insights

INTERVIEW

Cyber everywhere: Preparing for automotive safety in the face of cyber threats

An executive interview with GM's Jeff Massimilla

Tom McGinnis, Tom Haberman, Steve Schmith, and Ryan Robinson

The success of the interconnected automotive ecosystem may hinge on cybersecurity. GM's Jeff Massimilla speaks about what the company is doing to protect its operations, vehicles, and consumers from cyber threats, and how the industry is moving forward in its pursuit of cyber safety.

IN TODAY'S CONNECTED world, cyber is everywhere. This is particularly true in the automotive sector, where advanced, connected technologies are producing unprecedented disruption in almost every aspect of the automotive ecosystem, including manufacturing and supply chain, consumer engagement, connected and autonomous vehicles, dealer interactions, financing and, of course, enterprise operations.

With disruption often comes wide-ranging cyber risks for the automotive ecosystem. Cyberattacks can breach data, privacy, and safety; disrupt operations and compromise coveted intellectual property; cause financial losses; and dilute consumer trust in a brand. These are daunting challenges—but they also open up interesting opportunities. To gain insight on how automakers are approaching "cyber everywhere," we sat down with General Motors' (GM) vice president of global cybersecurity, Jeff Massimilla, to understand what GM is doing from an enterprise and product perspective to mitigate cyber risk.

"Understanding the different solutions and sharing knowledge across the industry are critical to address the rapidly evolving cyber threat landscape."

DELOITTE: How would you describe "cyber everywhere" in the automotive industry and how has it evolved over the past five years?

JEFF MASSIMILLA: The very concept of "cyber everywhere" has evolved greatly over the past five years. Earlier, it focused just on information technology systems, with the aim to prevent the loss of intellectual property. Even then, GM had a somewhat broader definition than other companies because of OnStar.[1] Today, however, cyber everywhere is truly an end-to-end connected ecosystem, from the back office through the telecom carriers and down to the platform itself, enabling automated driving and convenience features, mobile hotspots, and so on. GM still has an information security function, but it has evolved to be highly focused on data privacy. Focus has also moved to the manufacturing environment, the most recent evolution of cyber everywhere across most industries. Insulating manufacturing from disruption, while protecting employees and product integrity, is all very important now. As a result, our cybersecurity organization is involved in every aspect of GM's business.

DELOITTE: How can automotive companies promote external collaboration to address cyber risks?

JM: Collaborations, whether within or outside of the automotive industry, are extremely important to understanding different solutions, and sharing this knowledge is critical in addressing the rapidly evolving cyber threat landscape. We collaborate with several industries including medical devices, aerospace and defense, and consumer electronics. The point of these relationships is to exchange knowledge and expertise around the key challenges in connected ecosystems. In the automotive industry, we have two very specific collaboration initiatives. The first is the US Auto Information

Sharing and Analysis Center (Auto-ISAC), which allows us to collaborate within a competitive industry. It encourages meaningful interactions among automotive companies with varying levels of cyber maturity. It provides a safe, trusted environment for participants to create best practices for the entire industry. The second critical piece is related to supply chain security—we work closely with our partner suppliers to ensure the integrity, security, and quality of our products. Collaboration presents some challenges too, with the main one being forming a *collaboration mentality* across the ecosystem, so that everyone is working together to mitigate the risks of cyber incursion.

"We try to share everything we can to bring the entire industry up, rather than compete on cyber."

DELOITTE: How do you navigate the threat of cyber risk to your business operations and products when you work with partners that might be operating in less mature cyber environments?

JM: Over the past few years, awareness of cybersecurity, as it applies to safety and privacy in the automotive industry, has skyrocketed. Regulation is not far behind either—the California Consumer Privacy Act, Europe's General Data Protection Regulation, various privacy regulations in South America, and regulatory activities on this front in China. The importance of having a strong cyber posture across these global markets cannot be overstated. Closer to home, at GM, cyber is a key priority and I'm impressed with, and appreciative of, GM's leadership in establishing maturity around cyber. GM's strong focus on cyber emanates from the CEO and her senior leadership team. We also have a cybersecurity committee within our board of directors. I truly believe that is the foundation for driving maturity in this space. Additionally, we try to share everything we can to bring the entire industry up, rather than compete on cyber. After all, cyber has to be done correctly, so that there is no risk to our customers or products.

DELOITTE: What sets GM apart in terms of its approach to cyber everywhere?

JM: There are varying levels of maturity among companies operating both within and outside the automotive space. Certainly, several organizations take it very seriously. There are also companies in the middle and some that have not prioritized cyber as an operational imperative. Large companies like us, that have the ability to attract the best cyber talent, have a responsibility to provide expertise, best practices, and tangible solutions to help smaller companies that struggle to get the right talent.

DELOITTE: Overall, how would you rank the industry's preparedness for the challenges of cyber today and how well do you think the industry is prepared for cyberattacks?

JM: The Auto-ISAC is foundational to the cyber preparedness of the auto industry and establishing trust among competing organizations. For example, if a major cyberattack puts customer safety at risk, we would tap into the Auto-ISAC structure to share updates and discuss mitigation strategies in real time because customer safety is most important in our industry. In addition, the Auto-ISAC is uniquely positioned to facilitate proactive incident-response exercises. We do this within our company all the time, but to do it as an industry—interacting with other stakeholders in the event of a cyber incident—is another level of preparedness.

DELOITTE: How is GM bringing consumers along in this cyber journey?

JM: We recognize that the increasing level of autonomy in vehicles can make cybersecurity a fundamental concern for our consumers. Yet in our

experience, consumers don't necessarily equate increasing vehicle connectivity with cybersecurity risk. Further, although data privacy is a concern, consumers may relate that more to the data and devices they bring into the vehicle. All that being said, we believe that overall consumer behavior and good cyber hygiene are a critical part of our ability to keep our consumers safe. For example, bringing a compromised smartphone into the vehicle could be problematic from a cybersecurity perspective. Therefore, we develop our products assuming that brought-in devices are already compromised and that consumers may be doing things in the vehicle that they should not be doing. As such, we develop our defensive posture with the central pillars of privacy and safety in mind.

Read our interview with GM's Mandi Damman, chief engineer of the autonomous vehicle program, to learn about how GM is bringing consumers along to build trust in self-driving and other advanced automotive technologies.

DELOITTE: What should car companies be prioritizing and what do you think are the most important things that need to happen to be successful in an evolving cyber ecosystem?

JM: Cyber is a rapidly evolving landscape and we certainly don't have all the answers, but we're focused and learning every day. First, cyber has to be a board-level priority, a CEO priority, and a priority within each function of the business because our industry is so interconnected. So, a top-down mandate will set the wheels rolling. Second, filling the massive talent gap in the industry is imperative for long-term success. The automotive industry and GM are competing with some of the most high-tech companies out there, including those in Silicon Valley. Overcoming the talent shortage by working with universities, government agencies, and other stakeholders is something the industry needs to do to be successful in the long run. Finally, it is incumbent upon larger companies to be proactive in helping the industry, so companies that do not have a similar ability to do everything on their own can have access to the knowledge and solutions that make the entire system stronger.

Cyber is a national security challenge and it is important to focus on it from an overall perspective. After all, you are only as strong as the weakest link in your ecosystem.

DELOITTE: How can companies achieve and accelerate top-down support from the board and senior executives?

JM: Company leaders have to show openness toward cybersecurity and an appetite for risk management. Their mutual willingness to do so is equally important. I think it also starts with the relationships being built among companies at the board, CEO, or cyber leader level. If those relationships exist, cross-pollination of ideas can occur. At GM, we are very interested in the whole industry moving forward together.

DELOITTE: Finally, do you have any thoughts on the key messages required to articulate the business case for top-down support?

JM: In today's digitally connected world, cybersecurity must be one of the top risks for any technology-dependent and forward-thinking company. The ramifications of a single cyber event could be catastrophic. So, recognizing the cyber risk and deploying the right mindset and resources are paramount. It's almost like having a permanent, post-breach mentality.

Editor's note: GM recently announced that Jeff Massimilla has been appointed to lead General Motors' Global Connected Ecosystem Integration group.

Stay tuned for our interview with Kevin Tierney, GM's chief product cybersecurity officer, as we delve deeper into what the company is doing to protect its vehicles, consumers, and others from cyber threats.

Mr. Massimilla's participation in this article is solely for educational purposes based on his knowledge of the subject, and the views expressed by him are solely his own.

Endnote

1. GM's subscription-based communications, in-vehicle security, emergency services, hands-free calling, turn-by-turn navigation, and remote diagnostics systems.

About the authors

Tom McGinnis | tmcginnis@deloitte.com

Tom McGinnis is a partner with Deloitte & Touche LLP. He has worked with clients across the United States and globally to deliver a wide range of projects including business strategy, tax structuring, ERP implementation, process improvement, cybersecurity, internal audit, and M&A. As the leader of Deloitte Risk and Financial Advisory's Safe Food practice, McGinnis leads the development of operational risk management approaches for safe food, which includes enterprise compliance, supply chain risk services, enterprise application integrity, crisis management, and analytics.

Tom Haberman | thaberman@deloitte.com

Tom is a Principal in the Deloitte Risk & Financial Advisory practice in Deloitte & Touche LLP. He has over 30 years of business process and information systems audit and controls experience. Haberman is an Automotive specialist within Deloitte's Consumer & Industrial Products industry business. In his role as principal with Deloitte Risk & Financial Advisory, Haberman serves as the lead business partner for one of the largest global automotive equipment manufacturers (OEMs). Haberman is responsible for delivering Deloitte's solutions to help organizations navigate business risks and opportunities – from strategic to reputational, financial to operational, and cyber and regulatory.

Steve Schmith | sschmith@deloitte.com

Steve Schmith leads marketing for Deloitte's Automotive practice globally and in the United States. He works with practice leaders and a team of marketers around the world to shape and activate marketing campaigns that drive the business and build Deloitte's brand with automotive stakeholders worldwide. He is also responsible for leading the practice's relationships with automotive trade groups, associations, and media groups across the United States.

Ryan Robinson | ryanrobinson@deloitte.ca

Ryan Robinson is the research leader supporting the global Automotive practice at Deloitte LLP. His primary focus is to create engaging, actionable insights to deepen the conversation around key trends and issues occurring across the global automotive sector landscape. For the past two decades, Robinson has supported companies throughout the automotive value chain from manufacturers and parts suppliers to private equity firms and after-market service providers. He has been a frequent speaker at industry conferences and has been quoted as a subject matter expert in major media outlets around the world. Robinson holds degrees in philosophy, classical archaeology, and English literature from Concordia University in Montreal.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Tom McGinnis
Partner | Risk and Financial Advisory
+1 313 396 3309 | tmcginnis@deloitte.com

Tom McGinnis is a partner with Deloitte & Touche LLP. He has worked with clients across the United States and globally to deliver a wide range of projects including business strategy, tax structuring, ERP implementation, process improvement, cybersecurity, internal audit, and M&A.

About the Deloitte Center for Cyber Risk

With human insight, technological innovation, and enterprisewide cyber solutions, Deloitte Cyber will work alongside you to help you find answers and solve for the complexity of each challenge, from the boardroom to the factory floor.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Kavita Saini, Aparna Prusty, Abrar Khan, and Anya George Tharakan

Creative: Kevin Weier and Rajesh Venkataraju

Promotion: Ankana Chakraborty

Cover artwork: Daniel Hertzberg

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, 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 finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever 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 States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.