Deloitte.
Insights

INTERVIEW

Cyber everywhere: Building cybersecurity, one vehicle at a time

An executive interview with GM's Kevin Tierney

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

GM's Kevin Tierney speaks about how the company is engaging its ecosystem on cybersecurity, navigating global regulatory environments, and how the industry is preparing to meet the host of potential cyber challenges.

CYBER IS AT the very heart of General Motors' (GM) vision of achieving its "zero crashes, zero emissions, and zero congestion" goal. Whether it's autonomous vehicles, increased connectivity, or electrified vehicles, technological innovation is now founded on software, which engenders inherent cyber risk. To address this risk and to help ensure consumer safety through its vehicles, GM is engaging in a meaningful dialogue with suppliers and other stakeholders.

We sat down with GMs' vice president of global cybersecurity, Kevin Tierney, to understand how automakers are approaching "cyber everywhere" and what GM is doing to mitigate cyber risks at the product level.

DELOITTE: How would you describe cyber everywhere in the automotive industry when looking at it through the lens of the work you do at GM?

KEVIN TIERNEY: I've been on the cyber journey at GM since 2013 and where the industry has gone since is pretty amazing. At GM, *cyber is everywhere*—it's in almost everything in the ecosystem. As such, we're deeply involved with our suppliers and our end-to-end manufacturing activities. Once you start to think about cybersecurity from a holistic perspective, you understand it really plays a central role in the company because it could impact many areas within most industries. When you take that seriously, it starts to permeate all aspects of your business.

DELOITTE: How has the industry's approach to cybersecurity evolved over the past five years?

KT: Driving detailed, technical cyber requirements through our supply base has been one of the fastest-growing trends in the industry. Every time we source a new electronic component, we extensively specify cyber requirements that are based on our "defense-in-depth" strategy. Establishing a collaborative feedback loop with suppliers to address cybersecurity concerns has been a particular focus of ours—it helps us understand the security posture of the components and systems going into our vehicles. Another key aspect of the cyber evolution is a dramatic shift away from "admiring the problem" to executing risk-mitigation protocols and being continually attentive to understand what's coming next.

DELOITTE: How do you go about collaborating across the entire ecosystem?

KT: There is no one-size-fits-all model for collaboration. We have forged strong relationships with our suppliers on the cyber front because they help us design, develop, and manufacture a number of components that go into our vehicles. Typically, we start a dialogue around cyber right when we start component-sourcing discussions. From that point on, there is daily interaction between groups as we develop and test each part.

Cyber risk tends to lurk in the nuts and bolts of the electrical system and software. Therefore, it's critical that we remain vigilant for cyber threats not

only across the industry, but also at a very granular level among our tier 2 and tier 3 suppliers. As a result, our cyber requirements have evolved considerably over time as we learn and get feedback from a broad base of stakeholders.

Cyber is something that we are all concerned about from a societal level down. The US Automotive Information Sharing and Analysis Center (Auto-ISAC) is an important conduit for collaborating across the industry. If I need to talk to someone at Ford or Fiat Chrysler Automobiles, I can call them directly, and that can be extremely beneficial for the industry as a whole. The Auto-ISAC's central commitment that *cyber security is not a differentiating factor* has helped build trust among members.

"The US Automotive Information Sharing and Analysis Center (Auto-ISAC) provides an environment where companies can engage in dialogue on security issues."

There is an opportunity for transparency on cyber among tier 1 suppliers given the fierce competition in that space. Nonetheless, there is already evidence of change on this front and I see it continuing to evolve in a positive direction over time.

As for dealers and other third-party service providers, we can't always control the environments our service tools operate in. As such, we maintain the security of our vehicle software update process through an end-to-end authentication that goes all the way down to the target module in the vehicle and back up to our servers here at GM. That's one very important control designed to take untrusted networks out of the risk equation.

DELOITTE: How prepared do you think the automotive industry is to tackle cyber risks today, and how well is it preparing for cyber risks on the horizon?

KT: The automotive industry has always taken safety very seriously and, as an industry, we equate cybersecurity and safety together. That said, you can never be 100 percent prepared for a cyber event no matter what you do. Even then, cyber planning and tabletop exercises go a long way in preparing you so that when a real event happens, you can react well.

In terms of the industry, I think we are in pretty good shape now, although I wouldn't say we're perfect. The fact that the US Auto-ISAC has been established and we've built some strong relationships is great progress.

DELOITTE: When it comes to the vehicle itself, what do you see as the largest cybersecurity concern?

KT: Connectivity continues to explode—every new feature has some degree of connectivity and software, and we're moving into this new world of technology where things are merging and evolving very quickly. Everyone likes to talk about vehicle-to-everything (V2X) connectivity, which is a big area of focus for us both here in the United States and in China, and this is where my concern lies. The biggest challenge is to develop solutions for each region that effectively address that region's distinct regulatory requirements without compromising on what we want to offer to our consumers. The proliferation of diverse cyber rules could be a big challenge in creating common global platforms in the future.

DELOITTE: What is the current state of the regulatory environment when it comes to cyber challenges in the automotive sector?

KT: We look at the regulatory environment through a global lens because we sell vehicles around the world and, depending on the market, we have to meet different levels of cyber requirements. These requirements are analogous to crash requirements and fuel economy standards where we have to be mindful of market-specific nuances. For example, there is an obvious focus on privacy, especially in California, so we are watching that very closely because our cybersecurity protection also helps to ensure data privacy. China is moving very fast on the regulatory front, focusing on specific parts of the vehicle, including the gateway and telemetrics modules, as well as on network security. It is certainly challenging to navigate some of these areas, but we are engaging in a dialogue with the help of our local manufacturing partner. We spend a lot of time understanding how this dynamic global regulatory environment will affect our products so that we can stay ahead of potential issues.

DELOITTE: What are the cyber implications of increasingly connected vehicles being built in new, autonomous "factories of the future"?

KT: There are quite a few electronic touchpoints between the vehicle and the manufacturing infrastructure. At some point during the assembly process, you have to hook up the battery and configure the software, which involves many security-critical protocols. We continuously monitor and evaluate what can be done automatically versus the intervention of manual processes on the assembly line to ensure key authentications and security provisioning are maintained.

"The automotive industry has always taken safety very seriously and we equate cybersecurity and safety."

DELOITTE: What are the top three things you would convey to another organization in terms of building a better, product-focused cyber program?

KT: First, cyber is a top-down strategic imperative. Leadership support makes it possible for any team to do the hard things that make a difference. Second, you have to get out there and find the best people that are curious and enthusiastic with a background that you can leverage and build on. Third, actively learn from others. Talk to other industries and figure out what you could be doing better because there just isn't a book on the shelf that tells you how to do automotive cyber.

DELOITTE: What does cybersecurity mean in terms of driving GM's vision of zero crashes, zero emissions, and zero congestion?

KT: The only way to achieve the "zero crashes, zero emissions, and zero congestion" goal is through connected, electronic, software-based systems. The same goes for advanced autonomous systems, V2X connectivity, and electric vehicles. These are all complicated, connected, electrical, software-based technologies. The focus on cybersecurity has to be there from the start; otherwise, customer safety may be compromised. In fact, cybersecurity is in the center of those three zeroes because without it, we simply would not be able to realize those technological innovations in a safe, secure manner.

"As the OEM, we need to make sure consumers feel safe and secure in the knowledge that we are doing the right thing on the cybersecurity front."

DELOITTE: How are you bringing consumers along on the cyber journey and building trust in GM's products?

KT: I think it is a very nuanced relationship and one that's evolving with time. Having personal control over the security posture of a car is different from, say, a laptop where you can have a lot of control. A car is purpose-built, so there isn't a lot a consumer can do to affect its security posture. As the original equipment manufacturer (OEM), we need to make sure consumers feel safe and secure. We do this by letting them know that we're focused on cybersecurity. If a consumer reaches out, our OnStar and other communication mechanisms answer questions and investigate any issues that they may have. As we move into the deployment of autonomous vehicles there will likely be more opportunity to directly engage with consumers on cybersecurity because I think it will be more relevant for them at that point.

DELOITTE: What are the largest cybersecurity concerns over the next three to five years that auto industry stakeholders should be focused on?

KT: As V2X connectivity is deployed at scale, we have to have a high level of transparency and collaboration across the entire global automotive industry. While the Auto-ISAC has helped, there is still more to do as an industry in terms of how we collectively move forward on cybersecurity. Additionally, organizations like the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) are working to create cyber standards. I think in the near term, OEMs might have different solutions for cybersecurity, which could present some challenges on the standardization front. Also, I think balancing cybersecurity requirements against the never-ending need to make innovative products that connect with consumers is an ongoing challenge.

Mr. Tierney'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. For more on what GM is doing in cyber and autonomous vehicles, be sure to read our articles featuring Jeff Massimilla, leader of GM's Global Connected Ecosystem Integration group; Kevin Quinn, director of GM's Additive Design and Manufacturing team; and Mandi Damman, formerly GM's chief engineer for their Autonomous Vehicles program.

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. He is based in Detroit.

Tom Haberman | thaberman@deloitte.com

Tom Haberman is a principal in the Deloitte Risk & Financial Advisory practice in Deloitte & Touche LLP. He has more than 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, Haberman serves as the lead business partner for one of the largest global original 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. He is based in Cincinnati.

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. He is based in St. Louis.

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. He is based in Toronto.

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

In an increasingly digital world, cyber brings new opportunities and threats. Our Cyber Risk services help clients address those threats to build smarter, faster, more connected futures. Using human insight, technological innovation, and comprehensive solutions, we manage cyber everywhere so society—and your organization—can go anywhere.

Deloitte.
Insights

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

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Kavita Saini, Nairita Gangopadhyay, Aparna Prusty, and Rupesh Bhat
Creative: Adamya Manshiva
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

About Deloitte