AUTOMOTIVE
CYBER SECURITY
SILICON VALLEY

AUTO-ISAC ON:

AUTOMOTIVE CYBER SECURITY TRENDS & CHALLENGES TO WATCH IN 2019

CONTRIBUTOR

Faye Francy, Executive Director, Auto-ISAC

Automotive iQ

FORWARD

Ahead of the **Automotive Cyber Security Silicon Valley Summit**, taking place this October 24-26 in San Jose, we sat down with conference chairperson, Faye Francy, to discuss the latest trends and challenges in automotive cyber security.

Faye Francy is currently the Executive Director of Auto-ISAC. In this position, Francy serves the global automotive industry through the analysis and sharing of trusted and timely cyber threat information about existing or potential cyber-related threats and vulnerabilities for on-road vehicle electronics and associated networks. The Auto-ISAC is a non-profit organization operating in Washington, D.C. Previously Ms. Francy was the Aviation ISAC Executive Director. She held numerous leadership positions at Boeing, including Cyber ONE Leader, Director Enterprise Technologies, Phantom Works and Air Traffic Management.

Faye Francy,
Executive Director,
Auto-ISAC

HOW DO YOU SEE THE ROLE OF ARTIFICIAL INTELLIGENCE IN AUTOMOTIVE CYBER SECURITY EVOLVING OVER THE NEXT FIVE YEARS?

Cybersecurity is an issue that many industries – including the auto industry – take very seriously. Connectivity and autonomy in the automotive industry are enabling safer, cleaner, more fuel efficient, and smarter vehicles. This makes vehicle cybersecurity a critical foundation for the future of the connected vehicle. Artificial intelligence is important for the success of autonomous vehicles and as such it is part of the cybersecurity threat landscape that automakers are addressing. Companies are examining artificial intelligence to support a robust cybersecurity program in the following ways:

1. **To accelerate incident detection**. In many cases, this means doing a better job of curating, correlating, and enriching high-volume security alerts to piece together a cohesive incident detection story across disparate tools.

HOW DO YOU SEE THE ROLE OF ARTIFICIAL INTELLIGENCE IN AUTOMOTIVE CYBER SECURITY EVOLVING OVER THE NEXT FIVE YEARS? *CONTINUED*

2. **To accelerate incident response.** This means improving operations, prioritizing the right incidents, and even automating remediation tasks.

3. **To help the organization better identify and communicate risk to the business**. AI can be used to sort through mountains of software vulnerabilities, configuration errors, and threat intelligence to isolate high-risk situations that call for immediate attention.

4. **To gain a better understanding of cybersecurity situational awareness.** In other words, CISOs want AI in the mix to give them a unified view of security status across the network.

Vehicle safety and security are our priorities, and automakers have long been working to reduce risks, and that includes steps taken from the very earliest vehicle design stages. Automakers voluntarily and proactively organize industrywide cybersecurity measures including establishing in 2015 an Information Sharing and Analysis Center (ISAC) that creates an industry-wide portal for sharing information and intelligence about existing or potential cyber threats. The Auto-ISAC will allow automakers to identify trends and common cyber threats more quickly.

ABOUT 40% OF ALL SUPPLIERS WE SURVEYED IN OUR 2018 AUTOMOTIVE TECHNOLOGY REPORT STATED THEIR MAJOR CHALLENGE AS CYBER SECURITY, COMPARED TO 34% OF OEMS AND 31% OF MOBILITY PROVIDERS. HOW DO SUPPLIERS CYBER SECURITY CHALLENGES DIFFER FROM OEMS AND MOBILITY PROVIDERS?

Since cybersecurity is everyone's responsibility, their challenge doesn't differ at all. It is incumbent upon each link in the supply chain to be engaged and vigilant in securing their part.

ABOUT 40% OF ALL SUPPLIERS WE SURVEYED IN OUR 2018 AUTOMOTIVE TECHNOLOGY REPORT STATED THEIR MAJOR CHALLENGE AS CYBER SECURITY, COMPARED TO 34% OF OEMS AND 31% OF MOBILITY PROVIDERS. HOW DO SUPPLIERS CYBER SECURITY CHALLENGES DIFFER FROM OEMS AND MOBILITY PROVIDERS?

CONTINUED

> The automotive industry and each individual company is only as strong as the weakest link. Cybersecurity is a global team sport and necessary to have all players on the field to thwart this nefarious threat and build automotive industry wide resiliency.

ADDITIONALLY, ABOUT A THIRD OF THE AUTOMOTIVE LEADERS WE SURVEYED IN OUR AUTOMOTIVE TECHNOLOGY REPORT LISTED THEIR MAJOR CHALLENGE AS 'CURRENT INFRASTRUCTURE IS NOT EQUIPPED FOR NEW TECHNOLOGY'. HOW WILL MAPPING THE ROADS IMPACT THE CYBER-RELATED THREATS AND VULNERABILITIES FOR ON-ROAD VEHICLE ELECTRONICS AND ASSOCIATED NETWORKS?

> Mapping the roads is just one element or supply function that is necessary for fully autonomous vehicles to be a success; sensors are another element. As each of these elements rely on networking and connectivity to operate effectively, they are subject to cyber-related threats and must be secured.
>
> Cybersecurity is an emerging threat with an adaptive adversary which means one must be vigilant. Automakers are committed to strong cyber security protections in the global connected vehicle ecosystem and working together to design in security at every level. This includes implementing security features during every stage of the design and manufacturing process, collaborating with public and private research groups to share solutions and participating in multiple cyber forums and activities on emerging issues.

WHAT WAS THE LARGEST CHALLENGE YOU/YOUR TEAM FACED OVER THE PAST YEAR AND HOW DID YOU OVERCOME IT?

"The single most important challenge: information sharing. Building trust is key. Understanding the mechanics of sharing and the processes in what, how and when to share is always a challenge in a highly competitive and diverse marketspace. Our motto is "share early and often" but that is easier said than done. The building blocks of trust and a shared information environment are essential. It is challenging for a company to share before it understands the full extent of the problem, and this can undermine sharing that might be beneficial for mitigation (if another member has already detected and perhaps solved the issue). The Auto-ISAC works with each member to ensure anonymity and we follow operating rules that each member's technical and legal teams have approved.

The trend for automotive cybersecurity is for greater collaboration and information sharing. Whereas, tremendous progress has been made over the recent years to get comfortable with information sharing, the industry has also recognized that there needs to be a redoubling of efforts in order to stay ahead of the ever-growing threats in order to detect and mitigate. Collaboration is a big benefit as members can learn from each other and quicken the speed of education for the whole of industry – one company's detection is another company's prevention. The Auto-ISAC membership develops best practices guides and conducts regular table top exercises to practice what, how and when to share.

The Auto-ISAC assists is members by socializing the value of information sharing and strengthening the collaboration with government, researchers, academia and other organizations. The Strategic Partner Program for the Auto-ISAC brings in valuable knowledge to transfer to the members and provides a learning platform for membership."

WHAT WAS THE LARGEST CHALLENGE YOU/YOUR TEAM FACED OVER THE PAST YEAR AND HOW DID YOU OVERCOME IT? *CONTINUED*

"The organization encourages members to establish vulnerability disclosure programs as these can be invaluable to organizations to help detect vulnerabilities and potential mitigation techniques. The Auto-ISAC, in partnership, with HackerONE conducted a vulnerability disclosure workshop in August to provide the tools and learnings of this valuable capability. This is a business best practice that improves the overall cybersecurity health of the automotive industry. The Auto-ISAC encourages security researchers to reach out to share information directly with the affected company or the Auto-ISAC as part of its partnership model.

The Auto-ISAC is the global industry's leading voice for cyber security, giving members a seat at the table where industry best practices and future governmental requirements are shaped. It serves as a central hub that allows members to share information and provide situational awareness across the industry to help effectively respond to cyber threats in real time."

AS THE CHAIRPERSON FOR THE UPCOMING AUTOMOTIVE CYBER SECURITY SUMMIT, WHAT IS ONE MESSAGE YOU HOPE ATTENDEES WILL TAKE AWAY FROM THE EVENT?

"Cybersecurity is everyone's responsibility."

Faye Francy, Executive Director, Auto-ISAC

CONTINUE THE CONVERSATION WITH FAYE AT THE SUMMIT!

AUTOMOTIVE CYBER SECURITY SILICON VALLEY

OCTOBER 24 - 26, 2018
SAN JOSE, CA

INTERESTED IN LEARNING MORE ABOUT THE LARGEST CHALLENGES FACING THE AUTOMOTIVE CYBER SECURITY INDUSTRY?

COMPLEX PROTECTION. RAPID RESPONSE.

The **Automotive Cyber Security Silicon Valley Summit** features leading cyber security experts working in automotive, mobility and parallel sectors. We will discuss key essentials like threat modelling, building in physical security, AI and deep machine learning, cyber security throughout the supply chain, and much more!

Cyber security has become an important differentiator between auto makers, mobility and other transportation companies as these industries are challenged with emerging and growing cyber security threats and challenges in increasingly complex security environments with connectivity, ADAS, and autonomous tech.

You will be able to network with other security professionals across several sectors and at various senior and technical managerial levels. In the past, this summit has attracted 100 + attendees from industry to top management from various OEMs and Tier 1 suppliers, such as CEOs, Presidents, Vice Presidents, and Directors of Engineering/Seating and solution providers.

LEARN MORE:

DOWNLOAD AGENDA

PURCHASE YOUR PASS

VIEW PAST ATTENDEE LIST

SPONSORSHIP OPPORTUNITIES