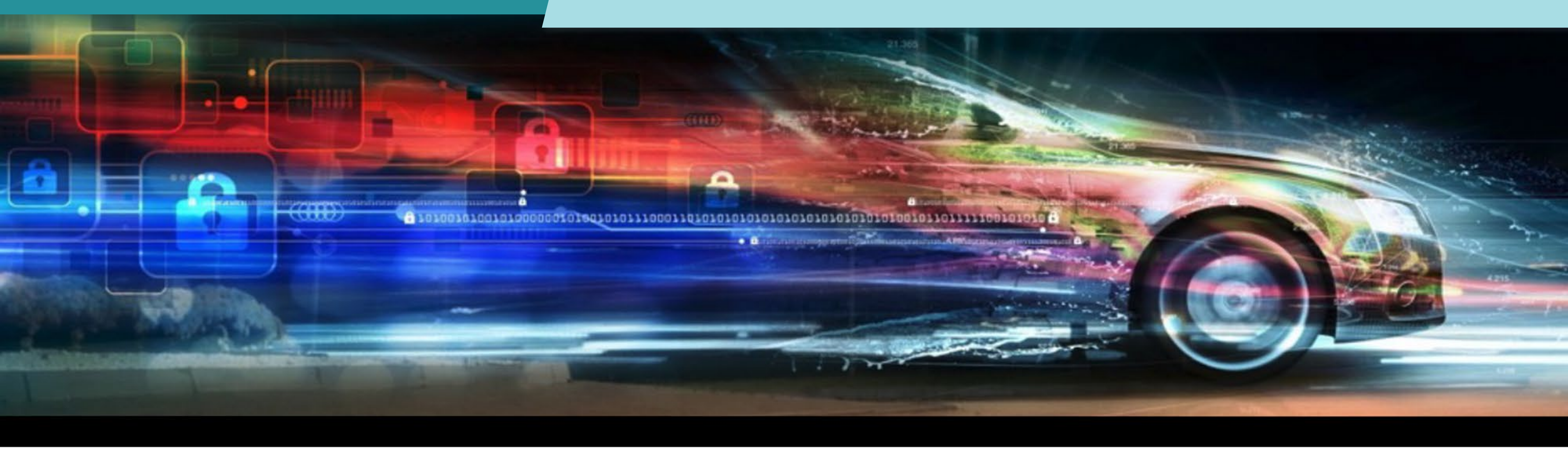


Welcome to Auto-ISAC!

Monthly Virtual Community Call

April 03, 2024

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Traffic Light Protocol (TLP)

Version 2.0 Definitions

Color		When Should It Be Used?	How May It Be Shared?
TLP:RED 🔴⚫⚫	**Not for disclosure, restricted to participants only.**	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT ⚫🟡⚫	**Limited disclosure, restricted to participants' and its organization.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ⚫🟡⚫	**Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ⚫⚫🟢	**Limited disclosure, restricted to the community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ⚪⚪⚪	**Disclosure is not limited.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We’re Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update*** ➢ **Jeff Terra, Joint Cyber Defense Collaborative (JCDC)**
11:20	**Featured Speaker:** ➢ **Darryn Persaud, CMO, Comply.Law** ➢ **Title: Automotive Cybersecurity Safeguards**
11:55	**Q&A & Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ ***Stay informed of Auto-ISAC activities***
- ✓ ***Share information on key vehicle cybersecurity topics***
- ✓ ***Learn about exciting initiatives within the automotive community from our featured speakers***

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – ***the whole of the automotive industry***

Classification Level:. Slides are at TLP:CLEAR and on our website. Discussions are TLP:GREEN & may be shared across Auto-ISAC Community, "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions! *"Cybersecurity is a Team Sport!"*

❖ Share – *"If you see something, say something!"*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

30 *OEM Members*

47 *Supplier & Commercial Vehicle Members*

21 *Navigator Partners*

20 *Innovator Partners*

Membership represents **99%** *of cars and trucks on the road in North America*

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

2024 Board of Directors

Thank you for your Leadership!

Kevin Tierney
Chair *of the*
Board of the Directors
GM

Josh Davis
Vice Chair *of the*
Board of the Directors
Toyota

Stephen Roberts
Secretary *of the*
Board of the Directors
Honda

Tim Geiger
Treasurer *of the*
Board of the Directors
Ford

Oliver Creighton
Chair *of the EuSC*
BMW

Andrew Hillery
Chair *of the CAG*
Cummins

Amine Taleb
Chair *of the SAG*
Harman

Maryann Combs
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

Auto-ISAC Member Roster

As of April 1, 2024

77 Members + 3 Pending

Aisin	Faurecia	Magna	Rivian
Allison Transmission	Ferrari	MARELLI	Stellantis
Amazon	Flex	Mazda	Stoneridge
American Axle & Manufacturing	Ford	Mercedes-Benz	Subaru
Aptiv	General Motors	Mitsubishi Electric	Sumitomo Electric
AT&T	Geotab	Mitsubishi Motors	thyssenkrupp
AVL List GmbH	Harman	Mobis	Tokai Rika
BMW Group	Hitachi (Astemo - Affiliate)	Motional	Toyota (Woven-Affiliate)
BorgWarner	Honda	Navistar	Valeo
Bosch (ETAS-Affiliate)	Hyundai	Nexteer Automotive Corp	Veoneer
Bose Automotive	Infineon	Nissan	Vitesco
ChargePoint	Intel	NXP	Volkswagen (Cariad-Affiliate)
CNH Industrial	JTEKT	Oshkosh Corp	Volvo Cars
Continental	Kia America, Inc.	PACCAR	Volvo Group
Cummins	Knorr Bremse	Panasonic (Ficosa-Affiliate)	Waymo
Daimler Truck	KTM	Phinia	Yamaha Motors
Dana Inc.	Lear	Polaris	ZF
Denso	LG Electronics	Qualcomm	
Deere & Company	Lucid Motors	Renault SAS	
e:fs TechHub GmbH	Luminar	Renesas Electronics	

Pending: Jaguar Land Rover, WirelessCar, SiFive

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

**All times are in ET

Auto-ISAC Business Updates and Events

- **Community Call:** Wednesday, May 1, 2024, **Time:** 11:00 – 12:00 p.m. ET TLP:GREEN **Speaker**: Walter Capitani, Director Technical Product Management, CodeSecure**Title:** "State of the Art Automotive SBOM Monitoring"

- **Auto-ISAC 2nd European Summit - BMW Welt in Munich, Germany:** June 12th – June 13th. The Titanium sponsor of the 2024 event will be BMW. Stay tuned for more details on our website.

- **ACT Fundamental Course Block:** Online, On-Demand $500/block
  - 3 Blocks: Cybersecurity Basics (32 hrs.) | Security Engineering (28 hrs.) | Security Operations/Management (22.5 hrs.)

- **Advance Course:** ***$2000 (Member Pricing), ($2250 Non-Member Pricing) with discount code.
  - Guided Attacks: April 29 - May 2, 2024, OPEN
  - CAPEX: Capability Exam is scheduled for May 22, 2024

- Auto-ISAC TLP:CLEAR 8th Annual Cybersecurity Summit will be held October 22 – 23, 2024

- Auto-ISAC's TLP:CLEAR 2nd Annual Auto-ISAC European Cybersecurity Summit will be held June 12 – 13, 2024 at BMW Welt in Munich, Germany.

AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

BMW GROUP

BMW WELT | MUNICH, GERMANY
JUNE 12-13, 2024

2024 AUTO-ISAC EUROPEAN CYBERSECURITY SUMMIT

SUSTAINING THE PRESENT – SECURING THE FUTURE

AUTO-ISAC SUMMIT

2024 Auto-ISAC Cybersecurity Summit

October 22-24 | Detroit, MI

In-person & Virtual

Information here

TLP:CLEAR

SECURE OUR STREETS CONFERENCE

19 SEPTEMBER 2024

HTTPS://SOS.ASRG.IO/

SECURE
OUR
STREETS
VEHICLE CYBER SECURITY

#SecureOurStreets

HTTPS://SOS.ASRG.IO/

HOW TO GET INVOLVED IN SECURE OUR STREETS

PRESENT

Be a part of the solution, present at SOS and help education and inform the community about your latest research, solutions, and demonstrations.

SPONSOR

Support the SOS Conference and **engage with the community** through our virtual booths and marketing opportunities.

ATTEND

Join the conference as a participant and learn together about automotive security challenges and solutions.

Participation is FREE

Auto-ISAC Intelligence Highlight

Ricky Brooks, Intelligence Officer

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- Know what we track daily: subscribe to the DRIVEN; TLP:GREEN Auto-ISAC 2024 Threat Assessment was released March 21 and we welcome your feedback.
  - **Send feedback**, intelligence, or questions to analyst@automotiveisac.com
- Intelligence Notes
  - Geopolitical tensions involving Russia, China, North Korea, and Iran remain **high** with Russia-Ukraine and Israel-Hamas in crises (Russia-Ukraine [1] [2], Israel-Hamas [3], Iran, China [4] [5], North Korea [6]).
  - Ransomware [7] [8] Groups Targeting Automotive: 8Base, Cl0p, BianLian, Black Basta, LockBit, Medusa, Play, Snatch
  - **Reminder:** malicious and non-malicious actors can explore, learn from, or leverage proofs of concept published on open-source repositories
  - **Notable Vehicle Research:** Truck-to-truck cyber worms via Electronic Logging Devices (NDSS); EV charger hacking (WSJ); LiDAR spoofing (NDSS); exploiting diagnostic protocols in embedded networks in commercial vehicles (NDSS).
  - **Notable TTPs and Tools:** Intentionally planting a backdoor in XZ Utils (Microsoft); Zenhammer (ETH Zurich); Exploiting TeamCity to mass-generate admin accounts (BleepingComputer); Malicious GitHub repositories (Ars Technica); Initial access brokers exploiting F5 BIG IP and ScreenConnect (Mandiant); Alleged insider threat leading to intellectual property theft (AP); BlueDucky (Mobile Hacker); StrelaStealer (Unit 42); Tycoon 2FA (Sekoia); Tiny Turla (Talos); StopCrypt Ransomware (SonicWall)

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Showcase a rich & balanced variety of topics and viewpoints
- *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

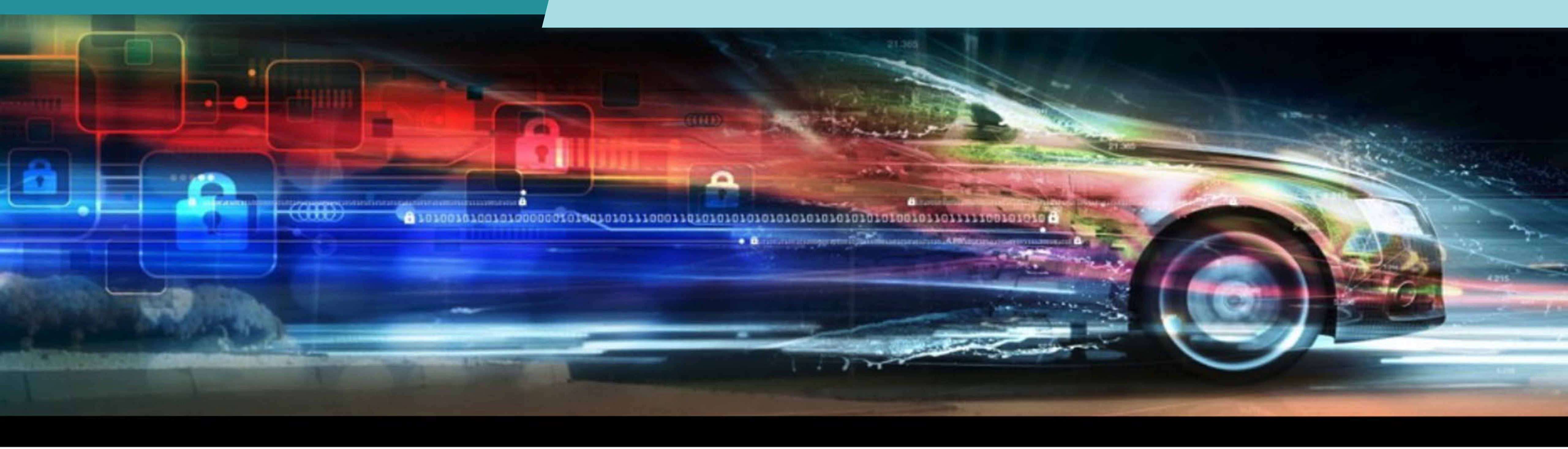
30+ *Featured Speakers to date*

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 *Best Practice Guides available on website*

2000+ *Community Participants*



Featured Speaker

Meet the Speaker

Darryn Persaud, CMO, Comply.Law

As a seasoned Digital Leader and Strategist, **Darryn** is an expert in over communicating product, process, and the design of customized advertising campaigns that integrate product into experience.

Darryn has worn many hats in his career; digital specialist, print, on air talent TV/Radio/Digital account executive, national account manager, strategist, planner. As a result, he has a unique ability to manage multifaceted projects and have navigated through complex business challenges.

Darryn harnesses over 15 years of experience in marketing and sales to drive the company's growth. His expertise lies in integrating innovative marketing tactics with solid sales strategies.

COMPLY.LAW

AUTOMOTIVE E-LEARNING WEBINAR

WWW.COMPLY.LAW

CYBER | SECURITY | TRAINING

QUESTION

How Can Dealerships Enhance Cybersecurity and Ensure Compliance?

Recommend regular employee training, cybersecurity audits and the adoption of strong password policies and secure network protocols.

.

Detail the implementation of security standards (e.g., NIST guidelines, PCI DSS compliance) to safeguard dealership data.

200,00
0

“The average company handles a bombardment of 200,000 security events a day”

$42,530

The FTC issues an administrative complaint when it has “reason to believe” that the law has been or is being violated. Each violation of such an order may result in a civil penalty of up to $42,530.

84%

The percent of cyber attacks due to human error (such as using easy-to-guess passwords, leaving physical devices in an unsafe areas, failing to apply a patch)

$3,590,00

The average cost for a data breach in the automotive industry as reported by Secure Code Warrior Report, August 2023

TESLA THWARTS RANSOMWARE THREAT

- Russian national tried to bribe Tesla employee
  - $1 Million offer
- Malware infection through thumbdrive/email
  - Download files for the criminals
  - Details of company networks
- Potential ransomware and data theft
- Employee reported incident to FBI
- Criminal arrested and charged

TOYOTA SUPPLY CHAIN ATTACK

Toyota suspended operations at 14 manufacturing plans due to a system failure at a supplier, Kojim Industries. This was due to a system failure at Kojima allegedly due to a cyberattack that prevent communications with Toyota. Kojima Industries provides plastic parts and electronic components to the automaker.

UBER HACK

Uber reported a third-party data breach as a result of a compromised vendor, Teqtivity. They track, monitor, and manage Uber’s IT assets and confirmed that data of more than 77,000 Uber employees may have been exposed to the attackers.

DEALERSHIP CHALLENGES

- A slew of new FTC Mandates applicable specifically to automotive dealerships
- The increasing digitization of the automotive industry has exposed automotive dealerships to cyber threats and regulatory compliance challenges
- Decentralized training platforms for various departments within dealerships
- Lack of employee retention and internal investment
- High internal training costs

$144,000

CBT News estimates that one underperforming service advisor
costs a dealership an average of 144K per year in unrealized profit

$10,000

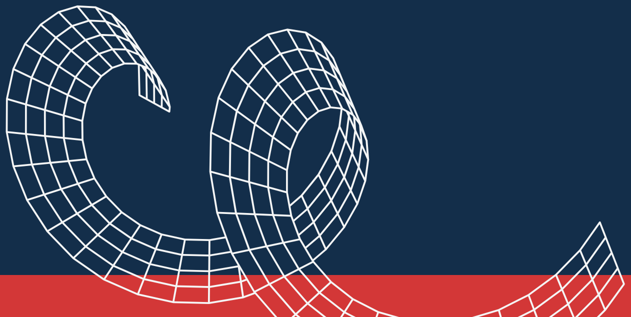
Dealerships have a 67 percent annual turnover rate amongst
it’s sales teams and the average cost of hiring a new dealership
employee is $10,000 (recruitment, onboarding etc .)

67%

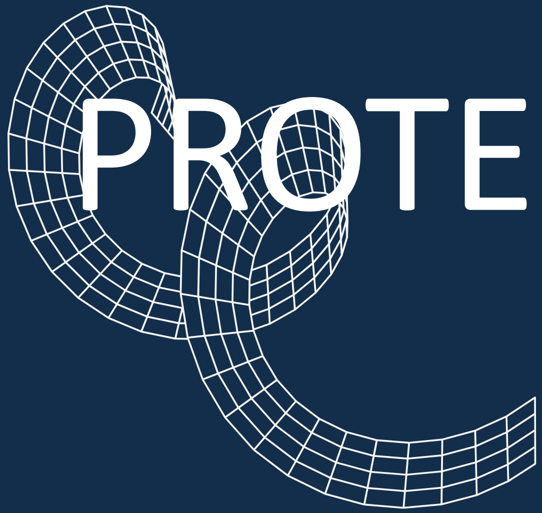
40%

Dealerships are sustaining an average 40 percent turnover rate across all departments

“The only thing worse than investing in people who don’t stay is not investing in people who do”



WHAT CAN YOU DO TO PROTECT YOUR DEALERSHIP?



HOLISTIC DEALERSHIP APPROACH

Identify & Manage Risks

- Cyber Security Governance
- Risk Management Frameworks
- Supply Chain Security

Protect Dealersip Ecosystem

- Layered Cyber Defences
- Information Protection Procedures
- Training and Awareness Programs

Detect Monitor and Respond

- Security Audits
- Vulnerability Management Plan
- Incident Management and Response

Quick and Safe Recovery

- Partnership Building and Information Sharing
- Cybersecurity as a process of continuous improvement

AUTOMOTIVE-CENTRIC BEST PRACTICES

Cybersecurity best practices should:

- Be built upon risk-based prioritized identification and protection of your dealership's employee's digital presence;
- Eliminate sources of risks by continuously training your employees
- Provide for timely detection and rapid response to potential cybersecurity incidents at your dealership;

AUTOMOTIVE-CENTRIC BEST PRACTICES

Cybersecurity best practices should (cont.):

- Design-in methods and processes to facilitate rapid recovery from incidents when they occur
- Institutionalize methods for accelerated adoption of lessons learned (e.g., vulnerability sharing) across the industry through effective information sharing, such as participation in Auto-ISAC.

HOLISTIC DEALERSHIP

- MODEL BEHAVIORS
- IDENTIFY BEHAVIORS
- SHARE IDEAS
- THREAT RISK ASSESSMENT
- MAKE HEROS
- FIND A LEADER
- CONNECT WITH YOUR SECURITY LEADER (S)
- KEEP AWARE

KEY TAKEAWAYS

- Full Organizational Approach
- Awareness of Risks and Threats
- Ongoing/Updated Employee Training
- Overall Governance of Cyber Risks, Financial Compliance Protocols, FTC Mandates and Employee Investment/ Retention

COMPLY.LAW TEAM

Henderson Chatargun

Chief Executive Officer
Co-Founder

Brings a dynamic blend of technology acumen, business savvy, and strategic thinking, cultivated over 15 years of launching and managing products in the B2B enterprise sector.

Darryn Persaud

Chief Marketing Officer
Co-Founder

Harnesses over 15 years of experience in marketing and sales to drive the company's growth. His expertise lies in integrating innovative marketing tactics with solid sales strategies

Suresh Maddula

Chief Technology Officer
Co-Founder

Seasoned IT professional with over 20 years of experience spanning technology, startups, and management. He specializes in transforming intricate business challenges into opportunities.

Brian Ramphal

Founder & Author

A seasoned expert in the intersection of technology and automotive dealerships, who boasts over 25 years of dedicated experience in the field.

AUTOMOTIVE
DEALERSHIP SAFEGUARD
CYBERSECURITY & FINANCIAL COMPLIANCE GUIDE
BRIAN RAMPHAL

THANK YOU!

VISIT WWW.COMPLY.LAW TO ENROLL YOUR DEALERSHIP

CYBER SECURITY (FTC MANDATED)

OSHA

SALES (PHONE & FLOOR)

FINANCIAL COMPLIANCE (FTC MANDATED)

HUMAN RESOURCES

ENVIRONMENTAL COMPLIANCE
(COMING SOON)

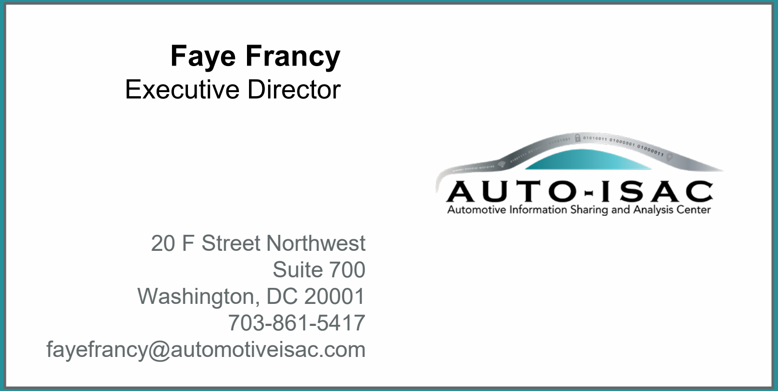
Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

Thank You

THANK
YOU
JUSPAXAR
OBRIGADO
MATONDO
SALAMAT
KIITOS
KIA ORA
MULTUMESC
MAAKE
MOCHCHAKKERAM
TERMA KASIH
RAIBH MAITH AGAT
MERCI
CHOKRANE
SALAMAT
CAM ON BAN
GRAZIE
MULTUMESC
MERCI
RAIBH MAITH AGAT
MERCI
OBRIGADO
MOCHCHAKKERAM
MOCHCHAKKERAM
GRAZIE
ASANTE
CHOKRANE
UA TSAUG RAU KOJ
MATUR NUWUN
MOCHCHAKKERAM
MATONDO
WELALIN
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
OBRIGADO
DANK JE
RAIBH MAITH AGAT
VINAKA
NIRRINGRAZZJAK
MAMANA
SPASIBO
SPASIBO
ARIGATO
KIITOS
MAAKE
DANKON
OBRIGADO
MOCHCHAKKERAM
NIRRINGRAZZJAK
MULTUMESC
MOCHCHAKKERAM
OBRIGADO
SPASIBO

Our Contact Info



Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street Northwest
Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM