21ST ANNUAL FREIGHT AND LOGISTICS SYMPOSIUM

Freight and Cybersecurity

A Summary Report | December 7, 2018 | Minneapolis, Minnesota

Sponsored by:
Center for Transportation Studies

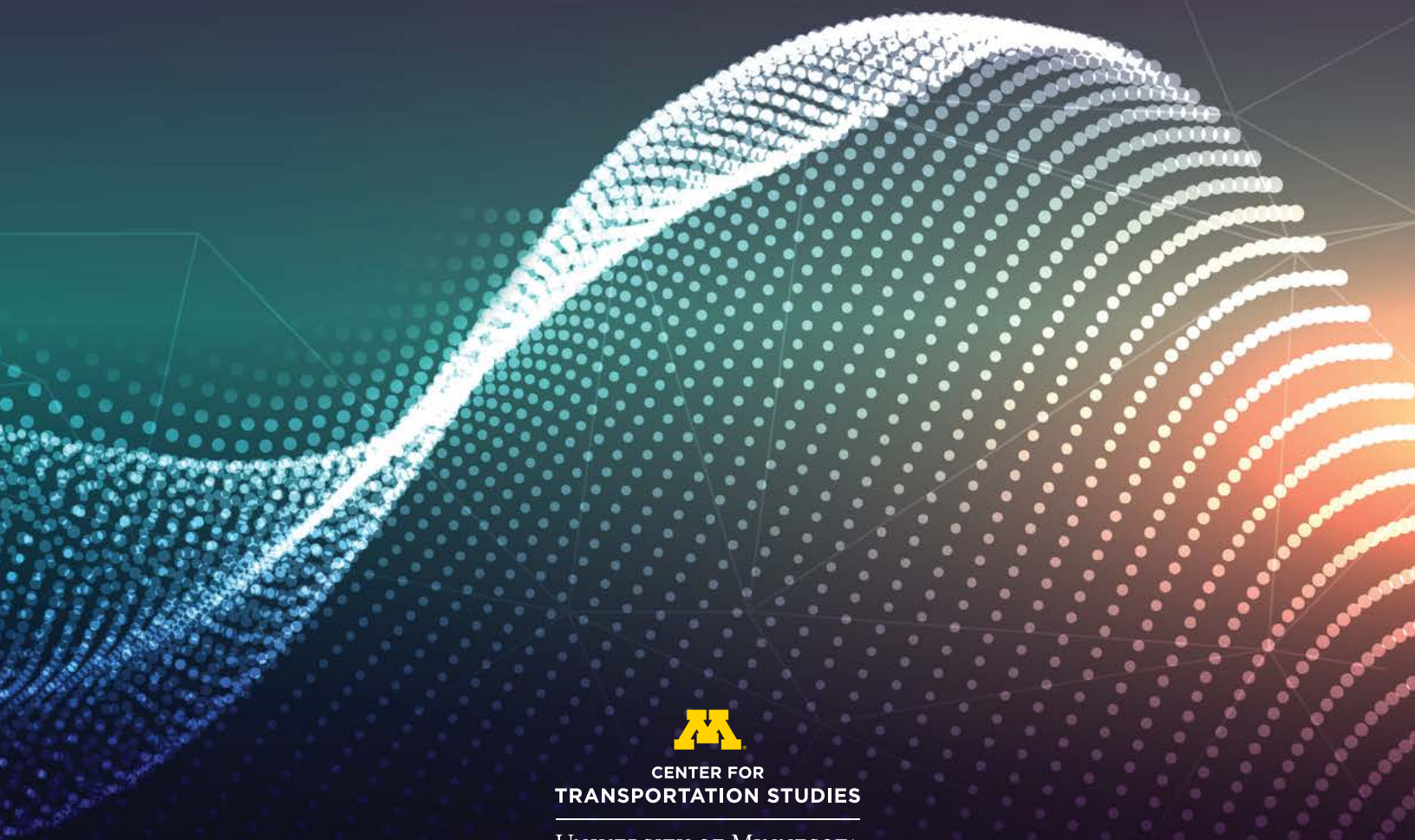
Facilitated by:
College of Continuing and Professional Studies, University of Minnesota

In cooperation with:
Minnesota Department of Transportation

Minnesota Freight Advisory Committee

Council of Supply Chain Management Professionals–Twin Cities Roundtable

Metropolitan Council



CENTER FOR TRANSPORTATION STUDIES

UNIVERSITY OF MINNESOTA
Driven to Discover℠

21st Annual Freight and Logistics Symposium

Freight and Cybersecurity

Cybersecurity has become a key concern for the freight and logistics industry in an increasingly connected and automated world. A significant challenge is balancing information privacy and security with the industry's need for usable, reliable data to produce expected benefits. In particular, potential improvements in safety, efficiency, and freight flow make it critical for Minnesota to invest in the development of connected and automated vehicles (CAVs) and tackle the complex cybersecurity issues that come with such progress.

Keynote: Using New Technology to Build Trust Across Supply-Chain Networks for Improved Transparency, Efficiency, and Security

- Leo Janus, Senior Offering Manager, IBM Watson Supply Chain

Panel: Cybersecurity and the Implications for Freight

Moderator: Meg Duncan, Director of Operations, Koch Logistics

Panelists:

- Brett Cooksey, Director of Technology, C.H. Robinson
- Rob Fischer, President, Geospatial Transportation Information Management Association
- Mike Johnson, Director of Graduate Studies, Technology Leadership Institute, University of Minnesota
- Augustine Moore, Minneapolis Area Port Director, U.S. Customs and Border Protection

Panel: Cybersecurity and Data Privacy Considerations for Connected and Automated Vehicles

- Jay Hietpas, MnDOT CAV Executive Director
- Josh Root, MnDOT Senior Legal Counsel and Data Practices Compliance Official

More information

Download this document and related materials from the 21st Annual Freight and Logistics Symposium: cts.umn.edu/events/freight/2018

Technological Advancements Benefit Supply Chains and Increase the Risk of Devastating Cyberattacks

Logistics giant Maersk paid $300 million to recover from a cyberattack not even directed at them. Starwood Hotels and Resorts took four years to identify a cyber breach affecting 500 million guests.

"Your chances of experiencing a cyberattack are increasing," said Leo Janus, senior offering manager with IBM Watson Supply Chain. "In fact, you are more likely to experience a data breach of at least 10,000 records than you are to catch the flu this winter. Statistically, it's becoming a very real thing, especially in logistics and supply chain."

New tech presents benefits and risks

As the featured speaker at the 2018 Freight and Logistics Symposium, Janus explored the potential of new technology to help fend off cyberattacks and build trust in supply chains while also increasing efficiencies. With 29 years of supply-chain experience, he currently taps a variety of technology tools to improve client supply chains.

But the application of more technology to benefit supply chains also increases the risk of cyberattacks that can devastate organizations, disrupt businesses, and result in significant losses to many stakeholders.

"How do we build trust when we're trying to digitize, and we're trying to create efficiencies?" he asked. "It's a difficult thing to do—knowing you could be hacked and attacked in a very short period of time by what's becoming more and more coordinated efforts to attack supply chains and systems and databases."

Cooperation and standards help counter cyberthreats

The rise in cyberattacks is helping bring diverse groups together in an effort to thwart future losses, Janus said. Recently, the global manufacturing giant Siemens led the charge at the 2018 Munich Security Conference to create a framework for dealing with trust and security.

Siemens and eight major global companies, including IBM, signed the resulting Charter of Trust, which establishes 10 key principles and calls for binding rules and standards to build trust in cybersecurity and further advance digitization. The charter also received support from government officials.

Applying standards, best practices, and processes also helps to ensure organizations are able to combat cyberattacks, he said.

The European Union has taken a strong position with industry and organizations to improve cybersecurity by establishing the General Data Protection Regulation to protect data and privacy.

"The whole intent here is to really bring some responsibility into data management," Janus said. "I think Europe is leading the way here."

The Internet of Things generates data

Technology continues to evolve at lightning speed. One example is the Internet of Things (IoT), a network of physical objects that can feed data.

IoT helps organizations understand what is happening in real time, make better predictions based on data, streamline processes, and gain efficiencies. In freight, for instance, electronic logging devices (ELDs) record data on trucks. IoT also becomes critical in a world with connected and automated vehicles (CAVs).

"With all the good things about IoT, there also are the threats," Janus said. Only a quarter of the participants in a recent survey were focused on IoT threat detection.

"You can't just use IoT without understanding that you also have to have a good program for security."

AI helps outthink cyberattackers

In addition to collaboration, standards, best practices, and cybersecurity initiatives, improved computing technology also may help thwart cybercriminals. For example, artificial intelligence (AI) literally learns from data inputs. Watson is the IBM machine learning and cognitive computing AI platform.

"AI is intended to ingest vast amounts of data, to reason over that data, and to learn from the interactions with that data—and then try to mimic human interactions," Janus said. "It's intended to help make better decisions or help understand situations better and put them into context."

When it comes to cybersecurity, AI can analyze data networks and detect anomalies, helping better understand attacks and outthink attackers.

Blockchain technology protects the supply chain

Another tool—blockchain—offers a private platform that encourages trust among multiple partners to share information and complete transactions. Blockchains require permissions, which means parties in the blockchain only access data that is relevant to their work.

A new trade and freight-related blockchain entered the marketplace in 2018. Maersk and IBM collaborated to conceive TradeLens, which is designed to apply blockchain to the world's global supply chain. More than 90 organizations have agreed to participate in the TradeLens platform.

TradeLens uses IBM blockchain technology as the foundation for digital supply chains. It allows multiple trading partners to collaborate by establishing a single shared view of a transaction without compromising details, privacy, or confidentiality. It gives shippers, shipping lines, freight forwarders, port and terminal operators, and inland transportation and customs authorities real-time access to shipping data and documents, which increases efficiencies and streamlines business processes. And it operates in a secure environment that uses the protection of digital keys and certification.

AI and automation make it possible to identify and contain breaches as much and as quickly as possible. The value of open collaboration between government and industry also can't be overstated. "We need to learn, and we need to coordinate," Janus said, "because the cyberattackers are coordinated."

"You are more likely to experience a data breach ... than you are to catch the flu this winter. Statistically, it's becoming a very real thing, especially in logistics and supply chain."

–Leo Janus, IBM Watson Supply Chain

Cybersecurity Has Become Essential to the Supply Chain

Cyberattacks ranked as the third-most-likely global risk for 2018, behind extreme weather conditions and natural disasters, according to the World Economic Forum. Prevention involves understanding where most cyberattacks begin.

"Roughly 93 percent of all successful breaches start with a phishing attack," said Mike Johnson, an expert in security technologies with the University of Minnesota Technological Leadership Institute. "If you want to look at one thing other than your vendors to do personally, make sure you're not subject to a phishing attack."

Johnson was one of four experts on a symposium panel to explore how the freight industry can make its data systems and processes more secure from increasing threats. Johnson was joined by C.H. Robinson technology director Brett Cooksey, Geospatial Transportation Information Management Association president Rob Fischer, and Augustine Moore, Minneapolis-area port director with the U.S. Customs and Border Protection (CBP). Meg Duncan, director of operations for Koch Logistics, moderated the discussion.

Increased risk requires increased security

"There is a huge drive to implement technology," Johnson said, observing that with drive often comes increased risk. "When you increase risk, you also have to increase planning for security."

Manufacturing and supply-chain industries are increasingly becoming aware of those risks. Responding to them, he said, requires incorporating strategies and solutions into your business model, rather than adding security options after an incident.

Engaging and listening to others also plays an important role in finding new effective approaches. "As leaders," Moore said, "we should be open to new ideas, allow people to own a process, and also take some risks."

Effective communication and coordination are vital

Effective communication and coordination can make a difference in preventing cyberattacks and improving cybersecurity.

Because companies often can be hesitant to communicate about security breaches and other concerns, the federal government created Information Sharing and Analysis Centers (ISACs) to encourage industry-specific information sharing, Johnson said. Organizations sign non-disclosure agreements to participate, which helps members talk openly about their security issues and solutions.

Concerns about damage to the company's image, liability questions, and impact on stock prices make it more difficult to share information. "Organizations are more willing to share operational aggregate data," Johnson added. "There's a reluctance to share cyber data unless there are protections in place."

The auto industry has a long history of forming trade associations and members also participate in the auto ISAC, Fischer said. "They are sharing their experiences with threats and mitigation techniques."

Other resources include Information Sharing and Analysis Organizations, which were established to develop best practices across industries, and InfraGard, a nonprofit organization that forms a partnership between the FBI and members of the private sector. Those organizations help companies build relationships with peers and government agencies such as the FBI, Johnson said.

For C.H. Robinson, transparency is part of the company's security principles and protocols. "For us, it's not a disincentive. It's part of the process and procedure that we need to be totally honest in those cases," Cooksey said. "It's really focusing more on prevention and then being very proactive at it."

New technology still requires trust

With connected and automated vehicles (CAVs) on the horizon, the automobile industry is looking squarely at critical security questions as well, said Fischer, who also serves as interim executive director of the Megaregion Autonomous Vehicle Research Coalition.

"How is this car built?" Fischer asked. "How do you instill trust from the factory floor—all the sensors and components that go into a car—all the way through to the end user? That's a long supply chain."

Once produced, he added, how do you maintain a level of security throughout the vehicle's lifetime?

For the global company C.H. Robinson, technology and security strategy must consider laws and regulations throughout the world, Cooksey said. For example, when the company launched a new driver app to track the delivery of goods in Europe, additional steps were required to comply with the European Union's General Data Protection Regulation. Truck drivers in Europe, for instance, must opt in at a website each time they accept a load.

Third parties can increase risk

Third-party risk is a critical issue for all organizations in every industry, Johnson said. Studies show that 55 to 70 percent of successful breaches come from a third party.

"You've got vendors that are connected that have your data, and you can expect that 60 percent of the breaches that could occur to you will come from those sources," he said. "You are ultimately responsible. Vendors have to be at least as good as you are at security and hopefully better because they are handling your data."

At C.H. Robinson, vendors complete a robust security questionnaire as part of an evaluation process. "Security is not just technology," Cooksey said. "It's people, processes, and technology."

In particular, Cooksey checks if vendors have an individual committed to security and he also closely reviews their controls. "We go in with eyes wide open," he said.

Fischer agreed that it is important to identify and evaluate all threats, then work with those involved in the private and public sectors to mitigate risks.

To be sure, CAVs also pose some complicated issues, he said. To maximize the potential of CAVs, vehicles must be connected to the infrastructure, which means making sure all sensors are secure. "If you just focus on the CPU [central processing unit]," he said, "it's like locking the door and leaving the windows open."

Partnerships help protect the ports

With responsibility for 328 ports of entry, the U.S. Customs and Border Protection manages a significant flow of cargo traffic.

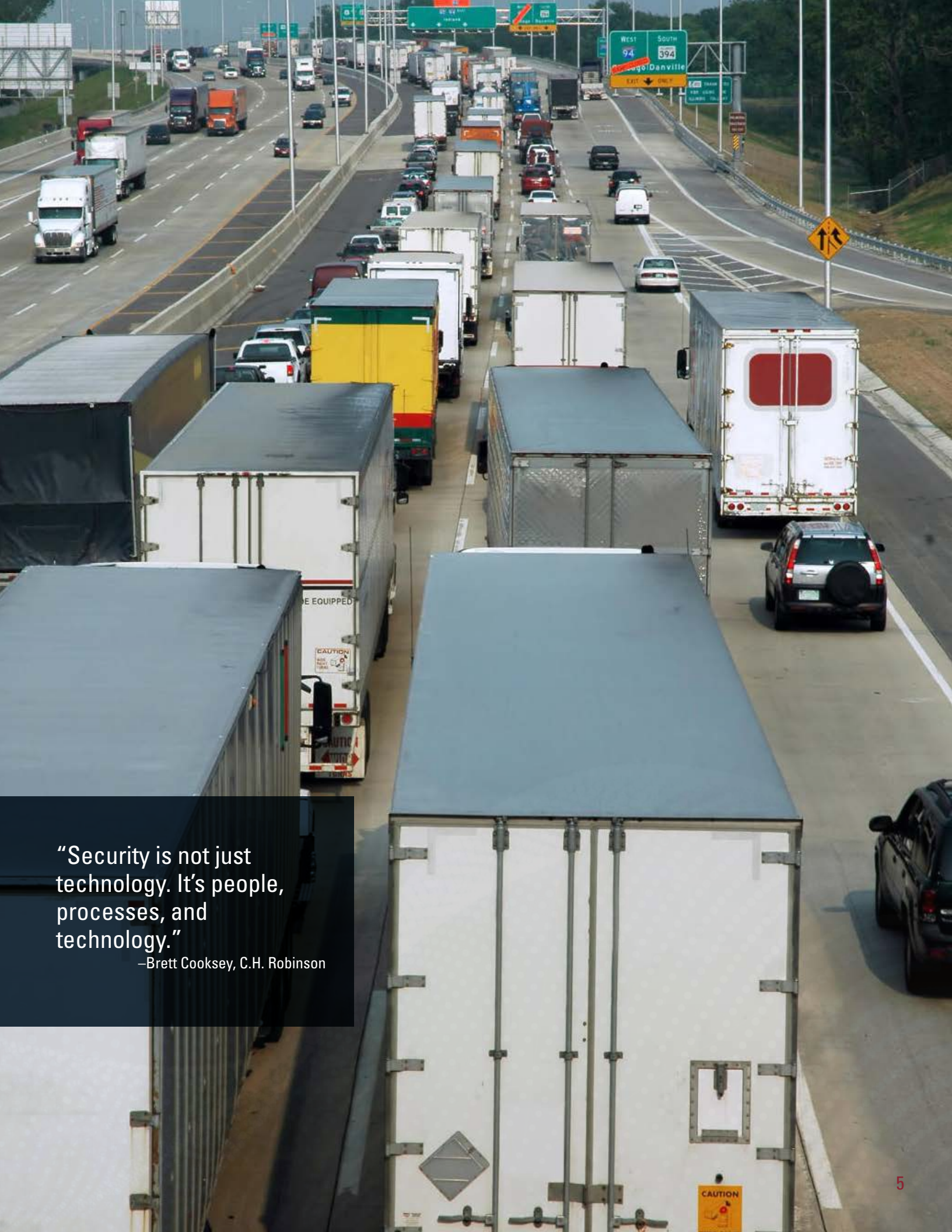
"When 9/11 occurred, we knew we had to change how we do business to ensure our homeland was safe," Moore said. "We worked with the trade community to build a program that would not stifle trade or movement of travelers."

The Customs Trade Partnership Against Terrorism (CTPAT) resulted from those efforts. "There is no such thing as no risk," Moore said. "But there is low risk."

CTPAT, a voluntary public-private program, helps CBP identify low-risk cargo by working closely with stakeholders of the international supply chain, such as importers, carriers, consolidators, licensed customs brokers, and manufacturers to support cargo security.

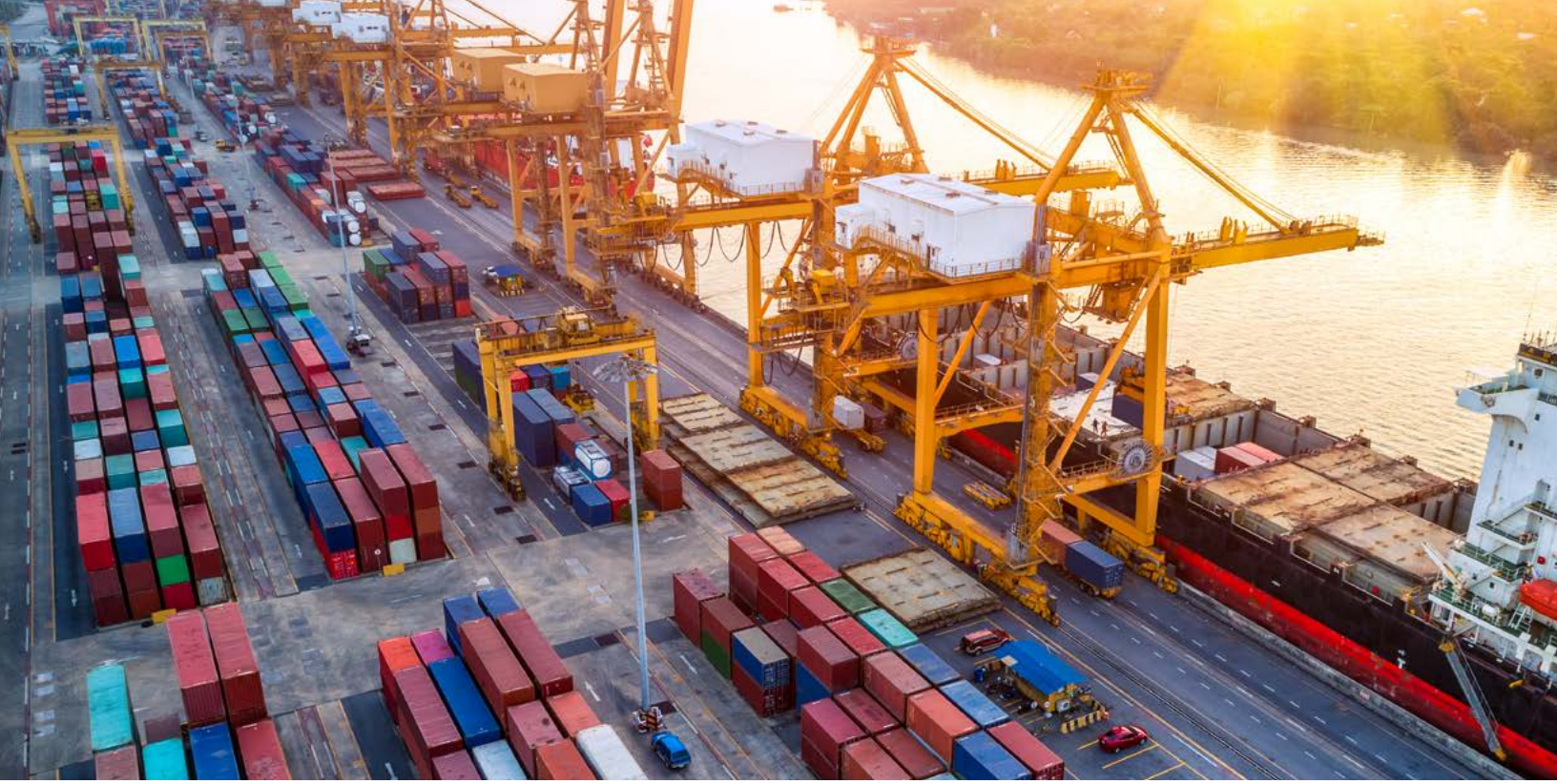
CTPAT organizations agree to collaborate with CBP to protect the supply chain, identify security gaps, and apply security measures and best practices. With those protections in place, CBP identifies partners as low risk—and less likely to be examined at a U.S. port of entry, Moore said.

In addition, the Automated Commercial Environment (ACE) helps automate all phases of cargo processing by allowing for the computerized submission of import and export documents. ACE also helps streamline trade processing by providing a system for data exchange between trade participants and CBP.



"Security is not just technology. It's people, processes, and technology."

–Brett Cooksey, C.H. Robinson



Cybersecurity and Data Privacy Top Concerns About Connected and Automated Vehicles

Connected and automated vehicle (CAV) technologies promise to improve safety, expand access and mobility, and increase efficiencies, according to Jay Hietpas, executive director of the MnDOT CAV-X office.

The possibility of CAVs on the road also raises many important issues, but security and privacy especially stand out in the minds of Minnesotans. "The public is very, very interested in this technology," Hietpas said. "We did a shuttle demonstration downtown, with 84 percent of people saying, yes, I want this technology. What was their biggest concern? Cybersecurity and data privacy."

State leads policy development

Hietpas and Josh Root, MnDOT senior legal counsel and data practices compliance official, concluded the symposium with presentations focused on cybersecurity and data privacy considerations for connected and automated vehicles.

A cybersecurity and data privacy policy subcommittee of the Governor's Advisory Council on Connected and Automated Vehicles, which included representatives from industry, academia, and government, took a broad look at the current state of the industry and the new security challenges that may result from further CAV development.

Root, a subcommittee member, emphasized the critical importance of cybersecurity to the development and implementation of CAVs. "Security is infinitely cheaper the earlier you work on it," he said. "Security built in or baked into our process is something that is an absolute must. It is a foundational element. It is something we have to do."

Uniform standards provide solid policy framework

The subcommittee and other stakeholders have stressed the importance of consistency in definitions and uniformity in standards. "One of the things we found through our process is that the definition of private is very different to most people than it is to a statute," Root said, highlighting the need for common terms.

Current statutes assume that drivers are human, but if a machine drives the vehicle down the road, then it becomes unclear who is liable in case of an accident and who carries the insurance—the human occupant or the manufacturer of the machine.

The effort to establish a uniform framework for all states and partnerships involved in CAV development best starts at the top, he said, and it will take time to build consensus. In addition, uniformity in security

standards will help make the system more affordable.

"If the security is not there and the security infrastructure is not working right," Root said, "these vehicles are not going to work right."

Partnerships help protect data and make it useful

CAV technologies can make plenty of data available, raising some serious questions about what, why, how, and where the data is being collected.

Most information that Minnesota citizens share with the government is not public according to the current definition of private data in Minnesota law. In the world of CAVs, though, that private data may prove helpful to industry partners in the further development of CAVs.

"So how do we do both?" Root asked. "Keep the information private while, at the same time, making your information anonymous and usable to the industry sector?"

It's important to be aware of those competing interests, to involve experts, and to pass legislation that makes sense for the long term, he said.

For Root, partnerships are the key to success, which means understanding what these partnerships need to thrive, what we are willing to share, and how we are going to share. "If we focus on what we need as opposed to what we want," he said, "it's going to be a lot easier for us to make those partnerships work and keep the public safe."

Stakeholder involvement is essential

Though the technology for driverless vehicles is developing rapidly, there are several more steps as well as cultural and educational barriers to overcome before launching driverless trucks. "There is a fear right now that these vehicles are going to be out on the road tomorrow," Hietpas said. "There's a long way [to go] before there are driverless trucks on the roadway."

Potential improvements in safety, efficiency, and freight flow make it critical for Minnesota to invest in CAV development, including tackling the complex cybersecurity issues that come with progress.

"Early-adopting states are going to win this race," Root said. "If we aren't going to lead, we're going to end up following. Let's get ourselves in a position where we can be part of that formulating group."

Stakeholder involvement in this initiative—including that of the freight community—is essential, Hietpas added.

An executive order in early 2018 required the state involve stakeholders, including representatives from

LEVELS OF AUTOMATION

Level 0 (No Automation)—The human driver performs all tasks.

Level 1 (Driver Assistance)—Technology assists the human driver by performing steering, accelerating, or braking tasks. Examples of Level 1 technology already available include adaptive cruise control and lane-keeping assist.

Level 2 (Partial Automation)—Technology assists the human driver by managing both steering and speed under certain conditions. These vehicles require the driver to monitor the surrounding environment, and are commercially available.

Level 3 (Conditional Automation)—In addition to Level 2 abilities, these vehicles can also monitor the environment. A licensed driver is still required to intervene and take control when the system notifies the driver. This technology is developed but not yet commercially available.

Level 4 (High Automation)—These vehicles are capable of operating with or without a steering wheel, pedals, or a human driver. These vehicles, in certain environments, can handle most driving tasks on their own. Limited level 4 vehicles are commercially available.

Level 5 (Full Automation)—These vehicles can drive, without a human driver, anytime, anywhere, and under any conditions. No level 5 vehicles are commercially available.

Source: Governor's Advisory Council on Connected & Automated Vehicles Executive Report (December 2018)

the freight community, in developing next steps for CAVs in Minnesota. Then, in December, the Governor's Advisory Council on Connected and Automated Vehicles issued a report recommending law and policy changes in support of CAV technology in Minnesota.

Proactive improvements offer competitive advantage

The order also delegated MnDOT to lead an interagency CAVs team and asked MnDOT, along with the Minnesota Department of Public Safety, to initiate testing and deployment programs when possible within current statutes.

"We are competing in a worldwide global market," Hietpas said. "If Minnesota doesn't come prepared, we're going to be at a disadvantage compared to other countries and other states that are actually enabling these technologies and using them for the benefit of their businesses."

Starting now also helps the state with planning for the changes that CAVs may bring, such as training and education and infrastructure adjustments.

"We know that there could be impacts to our infrastructure," Hietpas said. "So if we're not prepared and proactive in building out our infrastructure for these technologies, it's going to cost us more in the long run."

MINNESOTA FOCUSES ON TRUCK PLATOONING AS NEXT STEP FOR FREIGHT

Minnesota, led by the Governor's Advisory Council on Connected and Automated Vehicles, is moving closer to establishing a broader base of automated-vehicle regulations. Specifically for freight, the council is helping pave the way for truck platooning in Minnesota.

Truck platooning, which allows two or more trucks to travel in a convoy for increased safety and fuel efficiency, is gaining greater acceptance. Wireless technology enables the lead driver to control braking and acceleration for all trucks in real time, while drivers in each truck control steering.

So far, 23 states allow truck platooning, and 29 states have passed legislation on automated-vehicle testing. But current law is unclear whether automated vehicles and truck platoons may operate in Minnesota. Truck platooning is only legal in the state if the road authority designates a lane for use by trucks.

In December, the Governor's Advisory Council issued a report recommending that state law be changed so MnDOT and the Department of Public Safety can authorize truck platooning in collaboration with the public authority that has jurisdiction of the roadway.

In addition to truck platooning, the Governor's Advisory Council made recommendations for:

- safe automated-vehicle testing
- leadership and collaboration
- transportation and infrastructure
- vehicle registration, driver training, and licensing
- accessibility and equity
- revenue
- traffic regulations and safety
- insurance and liability
- cybersecurity and data privacy
- land use and planning
- economic development, business opportunity, and workforce preparation

The report calls for continued involvement by stakeholders, including the freight community. It will help guide policymakers as they consider changes in 2019 and beyond. Get more information and a copy of the report at dot.state.mn.us/automated.

Center for Transportation Studies
440 University Office Plaza
2221 University Avenue S.E., Minneapolis, MN 55414
612-626-1077 | cts@umn.edu | cts.umn.edu

Editor: Michael McCarthy **Writer:** Darlene Gorrill **Designer:** Angela Kronebusch
Photos: Shutterstock

"We know that there could be impacts to our infrastructure. So if we're not prepared and proactive … it's going to cost us more in the long run."

–Jay Hietpas, MnDOT