Accident Analysis and Prevention 203 (2024) 107644

Contents lists available at ScienceDirect

Accident Analysis and Prevention

journal homepage: www.elsevier.com/locate/aap

A simulator study assessing the effectiveness of training and warning systems on drivers' response performance to vehicle cyberattacks

Meng Wang [a], Jah'inaya Parker [b], Fangda Zhang [c], Shannon C. Roberts [a,*]

[a] Department of Mechanical and Industrial Engineering, University of Massachusetts Amherst, Amherst, MA 01002, USA
[b] Department of Industrial and Systems Engineering, University of Wisconsin-Madison, Madison, WI 53706, USA
[c] The Center for Injury Research and Policy, Abigail Wexner Research Institute at Nationwide Children's Hospital, Columbus, OH 43205, USA

ARTICLE INFO

Keywords:
Cybersecurity
Driver behavior
Driving simulation
Training
Warning systems

ABSTRACT

Modern vehicles are vulnerable to cyberattacks and the consequences can be severe. While technological efforts have attempted to address the problem, the role of human drivers is understudied. This study aims to assess the effectiveness of training and warning systems on drivers' response behavior to vehicle cyberattacks. Thirty-two participants completed a driving simulator study to assess the effectiveness of training and warning system according to their velocity, deceleration events, and count of cautionary behaviors. Participants, who held a valid United States driving license and had a mean age of 20.4 years old, were equally assigned to one of four groups: control (n = 8), training-only (n = 8), warning-only (n = 8), training and warning groups (n = 8). For each drive, mixed ANOVAs were implemented on the velocity variables and Poisson regression was conducted on the normalized time with large deceleration events and cautionary behavior variables. Overall, the results suggest that drivers' response behaviors were moderately affected by the training programs and the warning messages. Most drivers who received training or warning messages responded safely and appropriately to cyberattacks, e.g., by slowing down, pulling over, or performing cautionary behaviors, but only in specific cyberattack events. Training programs show promise in improving drivers' responses toward vehicle cyberattacks, and warning messages show rather moderate improvement but can be further refined to yield consistent behavior.

1. Introduction

Modern vehicles are monitored and controlled by numerous digital components (Eiza & Ni, 2017; Koscher et al., 2010) and are pervasively computerized. While this type of automotive revolution is designed to facilitate driving that satisfies one's increasing need for connectivity in the vehicle, consisting of robust internet connectivity either through embedded systems or mobile devices, it exposes vehicles to cyber-attacks. As more sophisticated services and communications features are incorporated into vehicles, the associated attack surface for modern automobiles is growing (Eiza and Ni, 2017; Khan et al., 2020; Koscher et al., 2010; Petit and Shladover, 2014; Zhang et al., 2019).

Vehicle cybersecurity has raised awareness about potential vulnerabilities. For example, two researchers used software to hack into a Jeep Cherokee in 2015 (Greenberg, 2015). In June 2016, a Mitsubishi Outlander was hacked by security researchers through manipulations between its mobile app and the Wi-Fi access point (Eiza and Ni, 2017; Zhang et al., 2019). Previous research also revealed that attackers were able to take control of the heater in Nissan Leaf electric vehicles via a mobile application, repeatedly turning it on and off (Eiza and Ni, 2017). Moreover, nearly 100 million Volkswagen vehicles that were manufactured between 1995 and 2006 were subject to remote, keyless-entry hacks (Garcia et al., 2016). It is important to note that real-world vehicle cyberattacks are relatively rare. While research has indicated potential vulnerabilities, they do not necessarily translate to everyday risks for the average driver as the frequency of actual attacks is not well-documented. However, the fact that researchers were able to identify and exploit these vulnerabilities demonstrates the need for continuous vigilance and improvement in automotive cybersecurity awareness.

The Federal Bureau of Investigation, with the U.S. Department of Transportation and the National Highway Traffic Safety Administration (NHTSA), jointly released a warning regarding the increasing vulnerability of motor vehicles to remote exploits (Eiza and Ni, 2017; FBI, 2016). The possible consequence of vehicle cyberattacks can range from malfunctions that could cause discomfort and distraction, such as the horn being activated, to fatal events, like the driver losing longitudinal

* Corresponding author at: Marston Hall 120F, 160 Governors Drive, Amherst, MA 01003, USA.
E-mail address: scroberts@umass.edu (S.C. Roberts).

https://doi.org/10.1016/j.aap.2024.107644
Received 19 June 2023; Received in revised form 17 May 2024; Accepted 18 May 2024
Available online 23 May 2024

or lateral control of the vehicle (Koscher et al., 2010). In such situations, if drivers are not aware of the abnormalities or do not take any actions, traffic safety would be further compromised and consequently, traffic crashes are more likely to occur.

While recommendations for improving vehicle cybersecurity have been made from the perspective of technology and system design (e.g., integrating all critical components into a single protected chip or vehicles only accepting the original software; Wolf et al., 2007), it is not feasible to design one security solution that fits all situations, especially given the randomness and uncertainty of vehicle cyberattacks. Since drivers directly interact with vehicles and will ultimately respond to any potential cyberattacks, it is equally important to consider the role of humans in this safety–critical loop (Cranor, 2008; Zhang et al., 2019). In addition, past research has suggested that solely relying on technology-based control over human behavior has not been successful in terms of minimizing the risk associated with cyber incidents (Pfleeger and Caputo, 2012). Cyberattackers will often take advantage of human users' naivete and careless behaviors to exploit unintentional vulnerabilities, which leads to the importance of bringing humans into the loop to reduce these vulnerabilities (Abawajy and Kelarev, 2012). Moreover, since vehicle cyberattacks can be sudden, unexpected, or in various formats, drivers would need to first notice what is happening and perceive the situations caused by vehicle cyberattacks to take more appropriate actions, per the definition of situation awareness (SA). In summary, one may not rely on technological solutions alone to improve vehicle cybersecurity; it is also important for drivers to gain awareness surrounding vehicle cybersecurity (Endsley, 1995b, 1995a; Wickens and Carswell, 2012). In the next section, we present the theoretical underpinnings for how drivers gain (and maintain) awareness of their environment.

1.1. Theoretical foundations

Operating a car imposes high cognitive demands on the driver (Unni et al., 2017). When facing an unexpected cyberattack event, the number and complexity of the elements in the driving environment are likely to increase, which would add another layer of difficulty for the driver to sense and understand the current situation. Furthermore, vehicle cybersecurity issues can be fatal not only because the vehicle could be controlled by others outside the vehicle, but also because drivers may not realize it is a cyberattack due to its rareness and fail to respond.

Information processing lies at the heart of human performance (Wickens et al., 2013; Wickens and Carswell, 2012). It begins with one sensing a stimulus, then interpreting it with some meaningful information, which requires attention resources – long-term and short-term memory – and finally completing response selection and execution. Central to information processing is the idea of transforming the perceived information into action, which highlights the importance of situation awareness (SA). SA is defined as "…the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future…" (Endsley, 1995b, 1995a; Wickens and Carswell, 2012). There are 3 states involved in SA: (1) perception of noticing, 2) understanding or comprehending, and 3) projecting or predicting (Wickens and Carswell, 2012). To have an effective decision-making process, it is essential for humans to maintain SA (Endsley and Connors, 2008). As such, Salas et al. argued that mental models are important for individual situational awareness (Salas et al., 1994). Mental models are defined as "the rich and elaborate structure which reflects the user's understanding about the system's contents, its functionality and the concept and logic behind the functionality" (Carroll and Olson, 1987, p. 12).

A correct mental model of vehicle cyberattacks and vehicle functions, which resides in one's long-term memory (a critical component in the information processing model), can interact with working memory to impact response selection when encountering vehicle cyberattacks. Such a mental model is also believed to be critical in predicting what might be happening in the near future, according to SA (Wickens and Carswell, 2012). Possessing a proper mental model of vehicle functionality and vehicle cyberattacks may increase the likelihood of a driver noticing and perceiving abnormalities caused by vehicle cyberattacks. That is, a proper mental model can benefit drivers in the context of vehicle cyberattacks in the phase of noticing and perceiving the environment, understanding the current situation and projecting the future, thereby leading to a positive contribution to their decision-making from the standpoint of both SA and information processing. Having a proper mental model of vehicle cyberattacks can also help drivers take the appropriate action after they become aware of the current situation. Many have highlighted that one has to have enough information and knowledge to be able to decide and that certain actions, such as slowing down and using the emergency brake, can be taken by the driver when encountering vehicle cyberattacks (McCarthy et al., 2014; Pfleeger and Caputo, 2012).

Putting it all together, vehicle cyberattacks are unexpected and rare events; as such, drivers are likely to respond slowly and inappropriately (Wickens and Carswell, 2012). Relatedly, human attention is selective and is knowledge-driven. A potential problem is that for those who are unfamiliar with vehicle cyberattacks, it may be challenging to notice and correctly perceive them. This can compromise both one's information processing and SA about current situations caused by vehicle cyberattacks. It also indicates a poor mental model of the situation.

In this study, we want to increase drivers' awareness of vehicle cyberattacks, improve their mental models of vehicle cyberattacks, and help them respond to such situations safely. That is, we hope to help drivers make better decisions and improve their performance when encountering vehicle cyberattacks based on principles of information processing, situation awareness, and mental models. More cautious behavior suggests that drivers exhibit greater safety awareness when facing a cyberattack event, in accordance with findings by Parker et al. (2022). More specifically, ideal responses to vehicle cyberattacks include slowing down, using hazard lights, shutting down network services, pulling over and shutting down the engine, or calling police or assistance for help to ensure safety, as highlighted in studies by Aliebrahimi and Miller (2023), Gemonet et al. (2021), Ouimet et al. (2013), and Zhang et al. (2019). Therefore, these actions were selected to represent an appropriate participant reaction to the cyberattack event in terms of safety awareness.

1.2. Training and warning systems

Training seems to be a natural and effective way to develop one's mental model of a system of interest. In addition to targeting drivers' mental models for improving their sensing and perceiving of the environment and long-term memory, providing warnings to assist their working memory and attention may also be helpful in enhancing their response performance towards vehicle cyberattacks (Wickens et al., 2013). Past research in the space of driving automation has found that appropriate interface design (e.g., warnings) and giving drivers knowledge about driving systems (e.g., through training) improves mental model development (Aziz et al., 2013; Feinauer et al., 2022; Krampell et al., 2020). In addition, both training and warnings have been shown to be effective means to positively influence driver behavior (Akhawe and Felt, 2013; Pollard et al., 2017; Roberts et al., 2021).

With respect to training, researchers have found that certain programs can help reduce young and inexperienced drivers' crashes (Roberts et al., 2021) and have been shown to improve drivers' responses to unexpected events (e.g., sudden acceleration; Pollard et al., 2017). Relevant research also supports this idea by demonstrating that when drivers know what to do, they can respond within seconds to unexpected and hazardous situations (Duncan et al., 1991; Soliman and Mathna, 2009; Zhang et al., 2019). In the field of cybersecurity, training has been shown to positively change user behavior and results in better recognition of faulty information (Cone et al., 2007). In addition, embedded

training has been found to effectively teach people how to avoid targeted cyberattacks (Kumaraguru et al., 2010). According to the Information Processing Model (Wickens et al., 2013), training leads to improved behavior because it elevates long-term memory and interacts with working memory, while also aiding in the process of perceiving the current situation. These together are likely to result in a better response selection and execution.

Warnings are also shown to be effective in improving drivers' behavior when they face unexpected events. Drivers who are given real-time information about a variety of behaviors such as fuel efficiency, driver distraction, and lane position quickly change their behavior (Birrell and Young, 2013; Dijksterhuis et al., 2012; Donmez et al., 2007). In regard to warning message design, it is suggested that symbols should have a clear relationship with the real-world to optimize comprehension (Lesch et al., 2011). In the field of cybersecurity, real time warnings about suspicious browser or smartphone behavior encourage safe behavior (Akwahe and Felt, 2013; Jedrzejczyk et al., 2010). In summary, both training and in-vehicle warnings can help increase drivers' SA and help correctly comprehend the situation when drivers encounter cyberattacks.

2. Research objective and hypothesis

While system design and preventative mechanisms, like firewalls and antivirus software, add an additional layer of protection against vehicle cyberattacks, training and warning systems that involve human drivers are an ideal complement that reduce vulnerability. As such, the goal of this study was to fill this research gap by examining whether training and warning systems improve drivers' response behavior to vehicle cyberattacks, as measured by the change in their velocity and acceleration (Gemonet et al., 2021) along with the frequency of engaging in cautionary behaviors (Classen et al., 2010). We conducted a driving simulator study to assess the objective. The hypothesis was that drivers who received vehicle cybersecurity training and in-vehicle warning messages would slow down, pull over, and exhibit more cautionary behaviors when they faced the cyberattack-induced events. More specifically, training and warnings would lead to: (1) a reduction in velocity, (2) a higher time proportion of large deceleration events (measured by elevated g-force values), and (3) more cautionary behaviors after a cyberattack-induced event occurs.

3. Methods

This research complied with the American Psychological Association Code of Ethics and was approved by the Institutional Review Board at the University of Massachusetts Amherst.

This study is a continuation of a previous study (Zhang et al., 2019). In the previous study, we focused on the iterative development of the training and warning systems using methods essential to human-centered design (e.g., interviews and co-design sessions). In this study, we assessed the effectiveness of the training and warning system in improving drivers' response behavior to vehicle-cyberattack-induced situations via a driving simulator experiment (Parker et al., 2022; Zhang et al., 2023).

3.1. Participants

A total of 32 participants (age 18–26) were recruited from the University of Massachusetts Amherst campus and the town of Amherst using flyers and The average age of the participants was 20.4 years (SD = 2.0 years). Only individuals with a valid United States driving license were included in this study. With respect to participant demographics, there were 23 males, 7 females, and 2 with a non-conforming gender. In terms of race/ethnicity, there were 28 Caucasian/Whites, 2 African Americans/Blacks, 1 Hispanic/Latino, and 1 Asian in terms of race/ethnicity. Last, there were 5 participants who drove less than 5000 miles in the past year, 10 who drove 5000–1000 miles, 12 who drove 10000–15000 miles, and 5 who drove 15000 + miles. A power analysis showed that with a sample size of 32 and an effect size of 0.38 when setting alpha to 0.05, the power is 0.8. The analysis was conducted for each drive, implying that alpha correction was not needed.

Participants were randomly divided into 4 groups with each group having the same sample size (n = 8): the control group, the training-only group, the warning-only group, and the training-and-warning group. Participants in the control group did not receive training, nor were they offered any in-vehicle warning messages. Those in the training-only group and the warning-only group received either the training or the warning messages, respectively. Participants in the training-and-warning group received both the training before the drives and warnings during the drives. An overview of the experimental design of the study is shown in Fig. 1.

3.2. Apparatus

The driving simulator was a fixed-based RTI (Realtime Technologies Inc.) consisting of a fully equipped 2013 Ford Fusion surrounded by six screens with a 330-degree field of view, as can be seen in Fig. 2. Ford Fusions offer the benefits of a midsize sedan with a handling and rank that are high among midsize sedans, therefore providing participants with a comfortable and familiar driving experience. The cab features two dynamic side-mirrors which provide realistic side and rear views of the scenarios for the participants. The interior of the car has a fully customizable virtual dashboard and center stack. Driving behavior data was directly recorded from the driving simulator at a rate of 60 Hz. Additionally, two cameras were used to record the hand and foot movements of the participant. The cameras were combined with the forward view and views of the dashboard via a program called Sim Observer (Fig. 3).

3.3. Roadway environment

Each participant drove 4 times: 1 baseline drive and 3 experimental drives. All drives share the same roadway environment (Fig. 4): a 2-way, 4-lane street in a rural-based area. The speed limit was 35 mph and there was moderate traffic. The roadway was designed in a simple and non-distracting way so that the cybersecurity events were salient. In the baseline drive, there was no unexpected, cyberattack-induced event, while in each of the experimental drives, participants encountered such an event. As can be seen in Fig. 4, the cyberattack occurred in the last straight section. This design was used to ensure that participants did not become over sensitized to the appearance of hazards (Ranney, 2011; Zhang et al., 2019).

3.4. Cybersecurity events

Because vehicle cyberattacks can manifest in various ways, multiple drives, each corresponding to a cybersecurity event, were used in this study. In the Siren drive, a siren, such as from a police car or an ambulance, played while there were no such cars anywhere nearby. In the Dashboard Signs drive, two common vehicle warning signs ("CHECK ENGINE" and airbag symbol) illuminated on the dashboard after a short beep, and they were repeatedly and randomly turned on and off. For the Lane Change drive, the participant's vehicle was suddenly controlled by the experimenter who made the vehicle weave between lanes. Each cybersecurity event lasted 2 to 4 s. All the cybersecurity events were adapted and developed based on past literature regarding the possible outcomes of vehicle cyberattacks (McCarthy et al., 2014). We specifically chose the three events because they are either safety–critical (Siren or Lane Change) (J. Garcia et al., 2020), representative of a cybersecurity event showing erroneous messages (Dashboard Signs), or lane positioning and navigation errors (Lane Change). During the experiment, the order of these events was presented from least to most

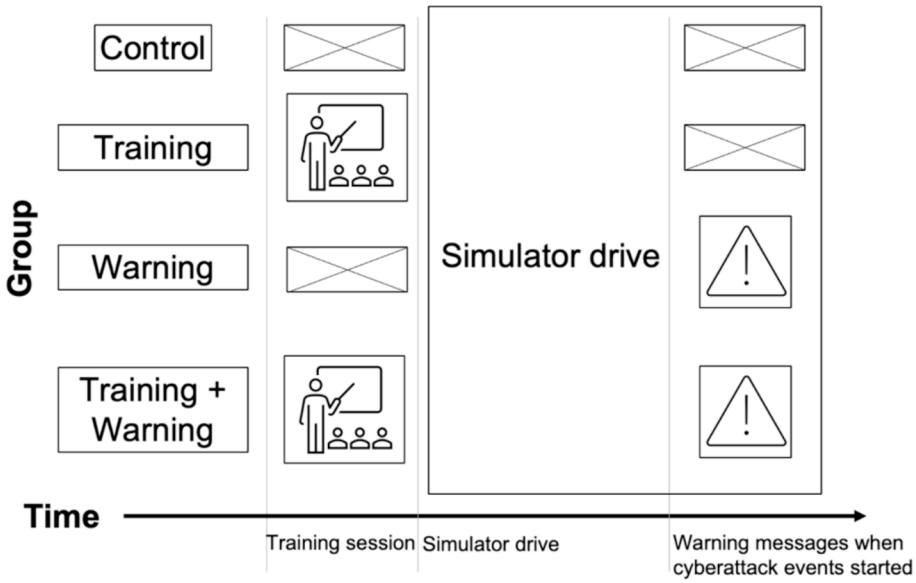

Fig. 1. The Experimental Design of the Study.

Fig. 2. Driving Simulator.

severe as to not bias the participant with an extreme event first, thereby significantly altering their response for subsequent drives. Therefore, all the participants experienced the same drive order: (1) Siren, (2) Dashboard Signs, and (3) Lane Change.

3.5. Warning messages

In phase 1 of the project (Zhang et al., 2019), we followed the human-centered design process – interviews and co-design sessions with participants – to collaboratively prototype and refine the design of the warning systems. The final content and format were finalized based on the results of a heuristic evaluation with four human factors researchers and the participants' feedback. The modality of the warning systems – auditory and visual – were preferred by most participants when asked about the ideal warning they would like to receive when vehicle cyberattacks occurred. In addition, we followed guidelines when designing the warning messages. First, in addition to the fact that the warnings of auditory and visual modality were preferred by the participants, it was also found to be the most helpful in past research (Maltz and Shinar, 2004). Second, command displays are most appropriate for the condition of high stress and time pressure (Lee et al., 1999; Wickens, 1992), so we used command sentences (e.g., drive with caution or slow down and pull over) to instruct participants.

When designing the warning messages, we categorized the Siren and Dashboard Signs as a non-safety critical situation and the Lane Change as a safety–critical situation. The warning messages were identical in the Siren and Dashboard Signs drives: a yellow warning sign showed on the dashboard right after the cybersecurity event. In addition, an audio message was played to notify participants that their comfort and convenience would be impacted. For the Lane Change drive, a danger warning sign and audio were provided, implying that the situation was more severe in nature. The audio message instructed them to slow down and pull over. Warnings were issued approximately 5 s after the cybersecurity event began. Each audio warning message lasted for around 2 s and was played from a speaker mounted in the vehicle so participants could hear and understand the message content clearly. Table 1 lists the cybersecurity event and the associated warning message.

3.6. Training program

Similar to the warning systems, the design of the training program was refined in phase 1 through the human-centered design process. Participants received a PowerPoint-slide-based training program where they were informed of the dangers of vehicle cybersecurity events, specifically, how to react if they fall victim. The training program was designed based on the 3 M (Mistake-Mitigation-Mastery) training method (Frese and Altmann, 1989), which has been successfully used to teach driving skills such as hazard anticipation (Roberts et al., 2021; Unverricht et al., 2018). This presentation consisted of a total of 12 slides. The first two slides provided examples of real-world vehicle cybersecurity incidents. The next two slides presented information about why vehicles were vulnerable to cyberattacks and what an attacker may gain from a vehicle cyberattack. Next, participants saw two slides about the outcomes of vehicle cyberattacks and what they should do in the case of a cyberattack. The participants were then tested on their knowledge using 5 different scenes (e.g., "What would you do if your vehicle changed lanes by itself?"), with each scene corresponding to one slide. They were considered finished with the scene once they correctly indicated the best reaction to the respective scene (e.g., check surroundings, slow down, or pull over; Chen et al., 2021; McCarthy et al., 2014). If they indicated an incorrect answer, the experimenter provided them with the correct answer. The five scenes were similar, but distinct,

Fig. 3. Sim Observer View.

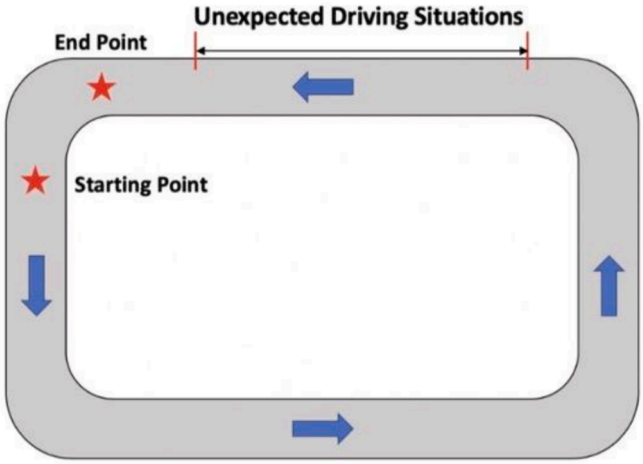

Fig. 4. Layout of the Drive.

from the examples provided at the beginning of the training program. The training concluded with a one slide refresher on how to react in the event of a cyberattack (Fig. 5). The training program was given before the simulator experiment and there was no time gap between the training program and the simulator experiment. The entire training program lasted between 10 and 15 min.

3.7. Study procedure

First, informed consent was obtained. Second, participants sat in the driving simulator and were instructed to conduct themselves as they would in a normal car. This includes adjusting the driver's seat, fastening their seat belts, adhering to the speed limit, using blinkers, and following any on-screen instructions. Third, participants took a practice drive to adjust to the simulator and controls. This was followed by the baseline drive in which participants drove through the same environment as in the experimental drives without any cyberattack-induced events. Fourth, if they were assigned to the training or training and warning group, participants underwent training (described above), which was used to help prepare them should they become a victim of a cyberattack. Drivers in other groups were instructed to drive in their usual manner, but not on how to behave when a vehicle cyberattack occurs. Participants then experienced the three experimental drives that contained the cybersecurity events. Regardless of group assignment the order of the drives was as follows: Siren, Dashboard Signs, and Lane Change. Each drive lasted 3–4 min. Once finished with the drives, participants completed a series of surveys in the following order: system usability survey (SUS) (Brooke, 1996), technology acceptance (Davis et al., 1989), driver behavior questionnaire (Reimer et al., 2005), sensation seeking questionnaire (Hoyle et al., 2002), and a post-drive questionnaire. Note that these surveys are not included in the current analysis. Finally, they were debriefed and compensated.

3.8. Dependent variables

Participants' behavior was measured by examining their velocity over time, the change in their velocity before and after the cyberattack event, and the proportion of time the driver had elevated g-force events (deceleration $>$ 0.45 g; Simons-Morton et al., 2012) after the cyberattack event started. These three dependent variables have been shown to be directly associated with driving performance and were therefore chosen to represent participants' response behavior from the perspective of safety (Aliebrahimi and Miller, 2023; Gemonet et al., 2021; Ouimet et al., 2013; Zhang et al., 2019). A reduction in the velocity and a larger time proportion of large deceleration after the cyberattack event is desired.

In addition to the driving data, we also examined video data by counting the times the participants checked the side mirror, checked the rearview mirror, and changed the number of hands on the wheel after the cyberattack event started. Taken together, we call these "cautionary behaviors". More cautionary behaviors suggest that drivers have better

Table 1
Cybersecurity Event and the Associated in-Vehicle Warnings.

Cybersecurity Event	Audio Warning Message (a female voice)	Visual Warning Message
Siren Siren similar to a police car or ambulance begins to play.	"Your comfort and convenience might be impacted. Distraction might be caused"	
Dashboard Signs A single high-pitched beep sounds and the two warnings signs illuminate on the dashboard in an alternating fashion. 	"Your comfort and convenience might be impacted. Distraction might be caused"	
Lane Change Experimenter takes lateral and longitudinal control of the vehicle, causing the car to repeatedly move from the left lane to the right.	"Your safety is compromised. Slow down and prepare to pull over"	

Fig. 5. Example Screen from the Training Program.

safety awareness when encountering the cyberattack events (Parker et al., 2022). To keep consistent time intervals, the before cybersecurity event period was defined as 5 s before the event started. On average, the post cybersecurity event period was 27 s.

3.9. Independent variables and data analysis

The main independent variables of interest were the training group (training, no training) and warning group (warning, no warning), which were between-subject variables. The within-subject variable was time (before and after the cyberattack event).

We employed mixed-design analysis of variance models (ANOVAs) on the velocity variables and Poisson regression on the normalized time with large deceleration events and cautionary behavior variables. To conduct the analysis, The normalized time with large deceleration events means that we normalized the time period and then counted occurrences of large decelerations over the normalized period. As a result, we consider that dependent variable to be the 'proportion of time with large deceleration events'. The ANOVA and Poisson regression model were built separately on the three drives: Siren, Dashboard Signs, and Lane Change. The formula of the Poisson regression model is as follows:

$$Y = e^{b_1X_1+b_2X_2+\cdots b_kX_k}$$

where Y is the dependent variable, and $X_i s$ are the independent variable. To conduct the analysis, the baseline drive was excluded from the analysis because it contained no cybersecurity events. Additionally, we only performed the Poisson for the proportion of time with large deceleration events for the period after the event as there were excess zeros in the period before the event (i.e., participants did not have a reason to slow down before the cybersecurity event). We performed a total of six mixed-design ANOVAs with velocity and change in velocity as the dependent variables and a total of six Poisson regression models

with the time proportion of deceleration and the count of drivers' cautionary behaviors. To account for the order effect where the participants were exposed to the same drive order during the experiment, all the analyses were conducted separately by drive.

4. Results

4.1. Descriptive Statistics

Table 2 presents descriptive statistics of participants' velocity by group based on drive and time. Across the Siren, Dashboard Signs, and Lane Change drives, participants who received training had a larger reduction in average velocity from before the event to after the event than the untrained group. No differences can be observed between the warning and no warning groups except in the Lane Change drive: those who received warnings had a larger reduction in velocity than those who did not receive warnings.

Compared to Siren and Dashboard Signs drives, participants in the Lane Change drive had a greater reduction in velocity from before the event to after the event. It should also be noted that in the Baseline drive, participants in all groups exhibited similar driving styles, i.e., no groups appear to intrinsically possess more careful or riskier driving behavior.

Regarding the proportion of time with large deceleration events (Table 3), those who were in the training group had the largest time proportion of large deceleration in comparison to other groups. We see the largest values for the proportion of time with large deceleration events after the event occurred in the Lane Change drive. However, in the Siren and Dashboard Signs drives, participants also had large decelerations when the cybersecurity event occurred, indicating that they acted by slowing down as a response to the event. In the baseline drive, participants did not have many large deceleration events. This naturally follows since there were no events in the drive, allowing participants to drive normally without the need to frequently or harshly apply the brakes.

Regarding the count of cautionary behaviors (Table 4), in the Siren group, participants had a larger number of these behaviors than in the Dashboard Signs and Lane Change groups on average. Participants who did not receive the training had more cautionary behaviors than those who received training whereas those who received the warning messages had more cautionary behaviors than those who did not receive warning messages.

4.2. Mixed design ANOVAs

4.2.1. Velocity

Table 5, Table 6, and Table 7 show the result of the mixed ANOVA model on velocity with time, training, and warning being the independent variables on the Siren, Dashboard Signs, and Lane Change drives, respectively. For the Siren drive, time and training were significant factors: after the event, participants decreased their velocity, with a greater reduction observed among those who received training. For the Dashboard Signs drive, there were significant time, training, and training * time effects. Combined with the visualization presented in Fig. 6, participants reduced their velocity more after the event when they received training compared to those who did not receive training. For the Lane Change drive, there were significant time and warning * time effects, suggesting a greater decrease in the velocity after the cyberattack event for those who received warning messages in comparison to those who did not. This trend can also be seen in Fig. 7.

4.2.2. Velocity difference between before and after the event

Similarly, the velocity difference between before and after the event was entered into an ANOVA with training and warning as the independent variables for each drive. There were no significant effects for the Siren drive. There was a significant training effect ($F(1, 26) = 5.113$, $p = .03$) for the Dashboard Signs drive and a significant warning effect ($F(1, 18) = 5.674$, $p = .03$) for the Lane Change drive.

It is worth noting that the ANOVA on the velocity difference is equivalent to a post-hoc analysis for the ANOVA on velocity. The results from the velocity difference analysis also match the results from the velocity analysis indicating that training was significant for the Dashboard Signs drive and warning was significant for the Lane Change drive.

4.2.3. Proportion of time with large deceleration events

The proportion of time with large deceleration events (in percentage) after the event was entered into a Poisson regression with training and warning being the independent variables for each drive. No training and no warning were the reference levels. For the Siren drive, Table 8 shows the output of Poisson regression. All factors including the intercept were significant. The results and Fig. 8 suggest that for those who were in the no warning and no training group, the expected proportion of time with large deceleration events was 15.18 %. For the single factors, the results imply that: (1) the expected proportion of time with large deceleration events for the training group is 1.65 times the expected time proportion for the no warning and no training group, and that (2) the proportion of time with large deceleration events for the warning group is 0.47 times the expected time proportion for the no warning and no training group. For the interaction factor, the results imply that: (1) for those who received training, the expected proportion of time with large deceleration events increases by a factor of 1.15 when comparing the warning group with the no-warning group, and that (2) for those who received warning messages, the expected proportion of time with large deceleration events increases by a factor of 4.01 when comparing the training group with the no-training group, implying that training was efficient, especially for those who received warning messages.

For the Dashboard Signs drive, Table 9 shows the output of Poisson regression. All factors, excluding the intercept, were significant. The results and Fig. 9 suggest that for those who were in the no warning and no training group, the expected proportion of time with large deceleration events was 1.12 %. The expected proportion of time with large deceleration events for the training group is 16.12 times the expected

Table 2
Descriptive Statistics of Velocity (in mph).

Drive	Time	Group							
		No training		Training		No warning		Warning	
		M	SD	M	SD	M	SD	M	SD
Baseline	Before event	39.92	4.88	38.58	5.11	38.80	5.55	39.92	4.33
Baseline	After event	43.93	4.71	43.49	5.04	43.04	5.84	44.15	3.52
Siren	Before event	41.48	3.90	38.58	4.97	39.69	5.44	40.36	3.70
Siren	After event	33.90	8.38	25.65	6.00	30.77	8.81	29.66	8.27
Dashboard Signs	Before event	39.92	5.08	38.36	4.08	39.03	5.40	39.03	3.84
Dashboard Signs	After event	39.03	5.98	32.11	7.72	35.46	7.98	35.68	7.60
Lane Change	Before event	39.03	4.37	39.25	4.82	38.80	4.88	39.47	4.28
Lane Change	After event	29.21	6.13	24.53	5.58	29.44	5.86	24.08	5.58

Table 3
Descriptive Statistics of the Proportion of Time with Large Deceleration Events After the Event.

Drive	Group							
	No training		Training		No warning		Warning	
	M	SD	M	SD	M	SD	M	SD
Baseline	0.01	0.031	0.003	0.013	0.01	0.031	0.003	0.013
Siren	0.111	0.116	0.266	0.117	0.2	0.151	0.172	0.128
Dashboard Signs	0.047	0.119	0.187	0.141	0.096	0.125	0.138	0.167
Lane Change	0.2	0.076	0.345	0.142	0.249	0.137	0.295	0.132

Table 4
Descriptive Statistics of Count of Cautionary Behaviors.

Drive	Group							
	No training		Training		No warning		Warning	
	M	SD	M	SD	M	SD	M	SD
Siren	8.25	6.34	4.6	2.35	6	5.6	7	4.68
Dashboard Signs	3	1.59	2.81	2.26	2.56	1.79	3.25	2.05
Lane Change	5.19	5.9	1.81	2.01	2.62	2.92	4.38	5.9

Table 5
Mixed ANOVA Result on Velocity for the Siren Drive.

Effect	DF numerator	DF denominator	F	p
Training	1	23	8.143	.01*
Warning	1	23	0.086	.77
Time	1	23	38.246	< .001*
Training * Warning	1	23	0.368	.55
Training * Time	1	23	3.67	.07
Warning * Time	1	23	0.416	.53
Training * Warning * Time	1	23	0.169	.69

(* $p < 0.05$).

Table 6
Mixed ANOVA Result on Velocity for the Dashboard Signs Drive.

Effect	DF numerator	DF denominator	F	p
Training	1	26	5.333	.03*
Warning	1	26	0.01	.92
Time	1	26	6.693	.02*
Training * Warning	1	26	0.638	.43
Training * Time	1	26	5.113	.03*
Warning * Time	1	26	0.082	.78
Training * Warning * Time	1	26	0.876	.36

(* $p < 0.05$).

Table 7
Mixed ANOVA Result on Velocity for the Lane Change Drive.

Effect	DF numerator	DF denominator	F	p
Training	1	18	2.596	.13
Warning	1	18	1.137	.30
Time	1	18	87.894	< .001*
Training * Warning	1	18	0.193	.67
Training * Time	1	18	1.212	.29
Warning * Time	1	18	5.674	.03*
Training * Warning * Time	1	18	0.303	.59

(* $p < 0.05$).

time proportion for the no warning and no training group. The expected proportion of time with large deceleration events for the warning group is 7.31 times the expected proportion for the no warning and no training group. For those who received training sessions, the expected proportion of time with large deceleration events increases by a factor of 1.07 when

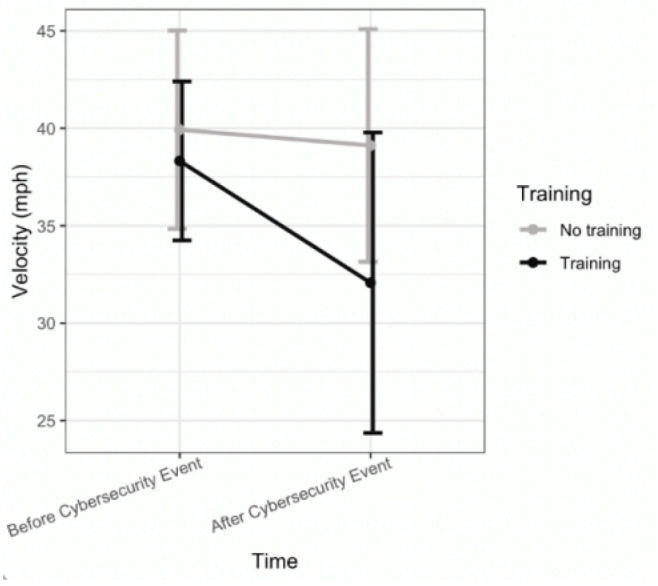

Fig. 6. Graph of Velocity (y axis) Before and After the Event (x axis) for Training and No Training Groups (line color) During the Dashboard Signs Drive; the Error Bars Represent the Standard Error.

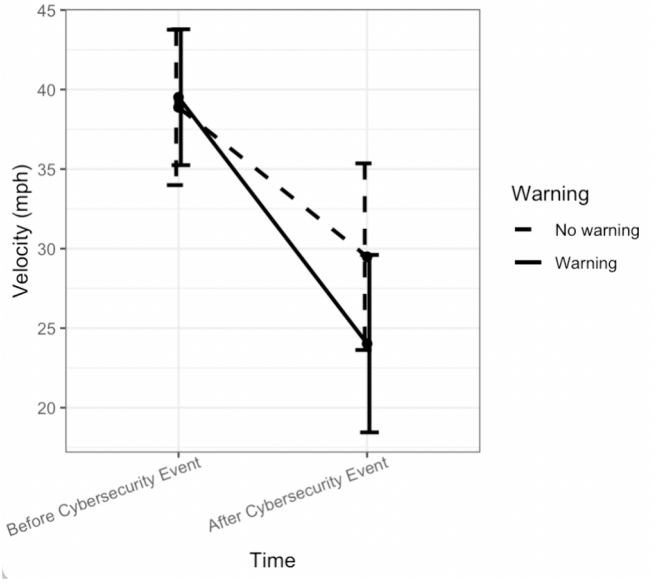

Fig. 7. Graph of Velocity (y axis) Before and After the Event (x axis) for Warning and No Warning Groups (line color) During the Lane Change Drive; the Error Bars Represent the Standard Error.

Table 8
Poisson Regression Result on Time Proportion of Large Deceleration for the Siren Drive.

Effect	Estimate	Std. Error	Expected Values	z value	p
(Intercept)	2.72	0.09	15.18	29.88	< .001*
Training	0.50	0.12	1.65	4.316	< .001*
Warning	−0.75	0.16	0.47	−4.686	< .001*
Training * Warning	0.89	0.19	2.43	4.708	< .001*

(* $p < 0.05$).

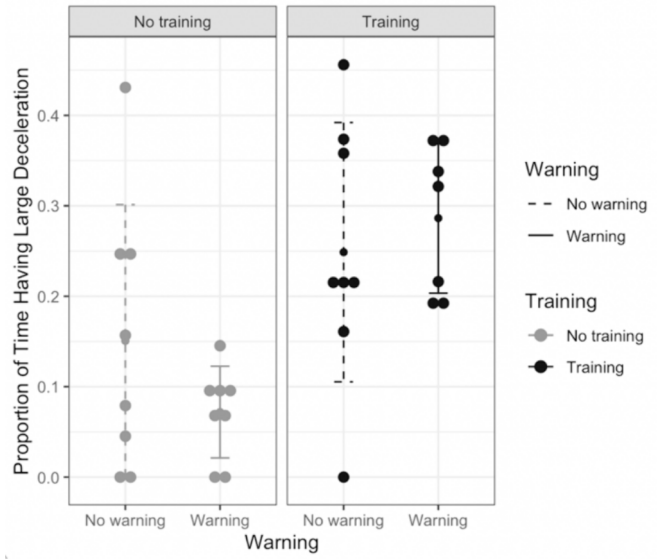

Fig. 8. Graph of Proportion of Time with Large Deceleration Events (y axis) Separated by Warning (x axis) and Training (grid) for the Siren Drive; the Error Bars Represent the Standard Error.

Table 9
Poisson Regression on Proportion of Time with Large Deceleration Events for the Dashboard Signs Drive.

Effect	Estimate	Std. Error	Expected Values	z value	p
(Intercept)	0.12	0.33	1.12	0.35	.72
Training	2.78	0.34	16.12	8.09	< .001*
Warning	1.99	0.36	7.31	5.61	< .001*
Training * Warning	−1.92	0.37	0.15	−5.14	< .001*

(* $p < 0.05$).

comparing the warning group with the no-warning group, implying that warning had little effect on those who had training sessions. For those who received warning messages, the proportion of time with large deceleration events increased by a factor of 2.36 when comparing the training group with the no-training group.

For the Lane Change drive, the results indicate that only training (*beta* = 0.52, $p < .001$) was significant. The expected proportion of time with large deceleration events for the training group is 1.65 times the expected proportion for the no warning and no training group.

4.2.4. Count of cautionary behaviors

The count of cautionary behaviors was modeled using Poisson regression with training and warning being the independent variables

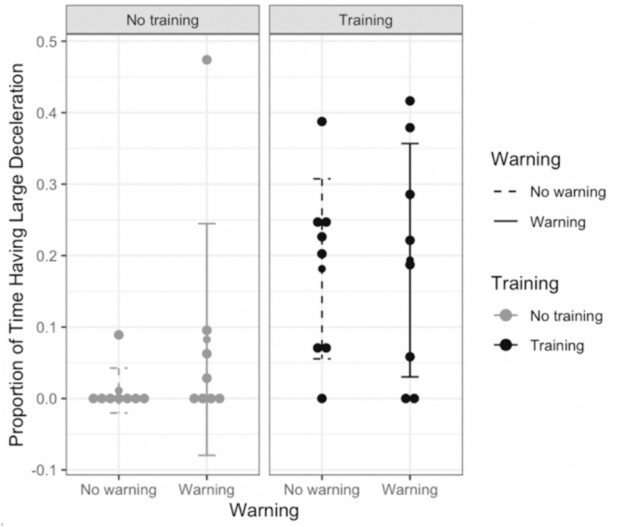

Fig. 9. Graph of Proportion of Time with Large Deceleration Events (y axis) Separated by Warning (lower x axis) and Training (grid) for the Dashboard Signs Drive; the Error Bars Represent the Standard Error.

separated by drive. No training and no warning were the reference levels.

For the Siren drive, there was a significant training effect (*beta* = −0.64, $p = .003$), indicating that the expected number of cautionary behaviors for the training group is 0.53 times the expected number of behaviors for the no warning and no training group. Training reduced the frequency of checking mirrors and/or changing the number of hands on the wheel.

For the Dashboard Signs drive, there were no significant effects.

For the Lane Change drive, the warning and training * warning interaction were significant. The results are shown in Table 10. The results and Fig. 10 suggest that for those who were in the no warning and no training group, the expected count of cautionary behaviors was 3 and that the expected count of behaviors for the warning group was 2.46 times the expected count of the behaviors for the no warning and no training group. For those who received training, the expected count of cautionary behaviors increases by a factor of 0.61 when comparing the warning group with the no-warning group. For those who received warning messages, the expected count of cautionary behaviors increased by a factor of 0.18 when comparing the training group with the no-training group, implying that training made the participants reduce the frequency of their cautionary behaviors.

5. Discussion

The present study focused on how Human Factors aspects can improve vehicle cybersecurity, which is an understudied topic, by analyzing whether a training program and in-vehicle warning message system help drivers respond to cyberattack-induced situations. A driving

Table 10
Poisson Regression Result on Count of the Behaviors for the Lane Change Drive.

Effect	Estimate	Std. Error	Expected Values	z value	p
(Intercept)	1.10	0.20	3.00	5.38	< .001*
Training	−0.29	0.31	0.748	−0.92	.36
Warning	0.90	0.24	2.46	3.72	< .001*
Training * Warning	−1.39	0.45	0.25	−3.07	.002*

(* $p < 0.05$).

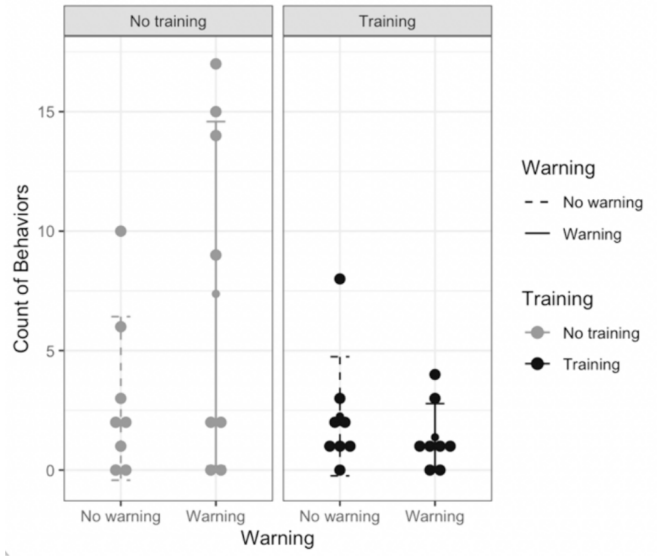

Fig. 10. Graph of count of cautionary behaviors (y axis) separated by warning (x axis) and training (grid) for the Lane Change drive; the error bars represent the standard error.

simulator study was conducted to assess the effectiveness of the training program and the warning message system on driver behavior, i.e., velocity, proportion of time with large deceleration events, and count of certain cautionary behaviors. Specifically, the research question was whether training and/or warnings would lead to enhanced driving performance, which in this case was reduced velocity, greater proportion of time with large deceleration events, and more cautionary behaviors (Gemonet et al., 2021).

Regarding the hypothesis focused on the effectiveness of training, the results of the mixed ANOVA on raw velocity suggested that the effect of training was most significant for the Siren drive as the participants in that drive generally drove at a slower velocity than the non-training group. In terms of the velocity difference, the effect of training was most significant for the Dashboard Signs drive as the participants reduced their velocity the most if they received the training sessions compared to the non-training group. The results of Poisson regression showed a significant training effect across all the drives, indicating that the participants had a greater proportion of time with large deceleration events when they received training programs. Additionally, those who received training performed cautionary behaviors less frequently after the Siren and Lane Change cyberattack events. Past research has found that training can improve people's hazard and risk perception (Duffy, 2003), but that was not necessarily the case here. When combined with the driving behavior results, it implies that training leads drivers to immediately react by slowing down, while also not looking around to gain information about their surroundings.

Concerning the effectiveness of warnings, the results of the mixed ANOVA on raw velocity suggest that the effect of warning was only significant for the Lane Change drive as participants in that drive generally drove at a lower velocity than the no-warning group. In terms of the velocity difference, the effect of warning was also only significant for the Lane Change drive as participants reduced their velocity the most if they received the warning messages compared to the no-warning group. Those who received warning messages after the cyberattack events are found to have a significantly greater proportion of time with large deceleration events for the Dashboard Signs drive and interestingly, less proportion of time with large deceleration events for the Siren drive. However, they also have more cautionary behaviors for the Lane Change drive. As the "pull over" warning messages were only provided in the Lane Change drive, it naturally follows that there is a stronger warning effect in terms of slowing down the vehicle and performing more cautionary behaviors. Taken together, it indicates that participants preferred to be thoroughly informed about what happened and what to do through a combination of visual and auditory warnings (Zhang et al., 2019) and that unclear warning messages (i.e., the non-safety critical events) will lead to a weaker, sometimes contradictory, effects (Parker et al., 2022).

Overall, the results indicated that training and warnings are effective in helping drivers respond to cyberattack events. Training programs seem to improve drivers' mental models, which helps them understand what cyberattacks are and what to do when they encounter a (suspected) vehicle cyberattack. Warnings are an important aspect in helping drivers understand the current situation and can present information effectively, thus improving drivers' decision-making ability (Endsley, 2015). Hence, drivers' situation awareness and understanding of vehicle cyberattacks are enhanced through training programs and warning messages. In addition, training on the comprehension of the warning symbols could help people's understanding of the situation (Lesch et al., 2011), indicating that the training and warning have a synergistic effect. It is worth noting that the training program instructed the participants on what the vehicle cyberattack was and what to do, and that the warning messages simply informed the participants of what to do. The stronger effect of training (over warnings) indicated that simply telling people what to do may not be effective, but rather giving them more information is more compelling (Aliebrahimi and Miller, 2023).

Relatedly, the effectiveness of training and warning are not consistent across drives. This more noticeable effect of training on performance and the rather moderate effect of warnings on performance could be due to a variety of factors. First, while much evidence has demonstrated training's effectiveness in enhancing driving performance (Casutt et al., 2014; Dorn and Barker, 2005; Roberts et al., 2021), other researchers have claimed that the effect of training on road safety is controversial, and that specific skills training has failed to promote measurable improvements (Dorn and Barker, 2005). Second, the impact of in-vehicle warnings on driver behavior is not always positive; their effectiveness depends also on other factors such as the time of issuance (Wan et al., 2016). Third, lack of understanding and comprehensibility of warning messages might be another factor that hinders people's performance and awareness. Providing training on the warning symbols and contents, as well as contextual cues to make the connection between the symbol and its referent can help people, especially older adults, better understand the warnings (Lesch et al., 2011, 2013).

For vehicle cybersecurity and traffic safety, in the future it is important to incorporate and implement appropriate training programs and warning systems on a larger scale. Training programs designed to educate both vehicle manufacturers and drivers can enhance cybersecurity vigilance. Manufacturers can incorporate secure design principles into their products, reducing vulnerabilities from the outset, while drivers can become more adept at recognizing potential threats and taking preventive actions. Meanwhile, advanced warning systems integrated into vehicles can defend against cyberattacks and alert drivers to potential risks in real time. As these systems become more advanced, they can detect and respond to threats autonomously, further improving the driving experience and safety for drivers. Implementing these measures on a larger scale not only enhances individual vehicle security, but also contributes to a collective improvement in automotive cybersecurity across the entire industry, making the road a safer place for all.

5.1. Limitations

Several limitations exist in the present study. The sample size was relatively small and the participants were all young drivers. Given young drivers' inexperience and lack of hazard anticipation, their response represents the least desirable option, implying that older, more experienced drivers would respond even better to training and warning than younger drivers. Future work should examine the effectiveness of training and warning systems with a larger group of more diverse

drivers. Also, only three vehicle cyberattack events were studied. Whether the results regarding training and warning systems' effectiveness in improving drivers' response behavior can be generalized to other situations and other driver groups remains unknown; more empirical evidence is needed. Additionally, with the limited cyberattack events, only the drivers' behavior was assessed, not their vehicle cybersecurity knowledge nor their mental models of vehicle cybersecurity. Third, temporal effects were not examined in this study, e.g., it is unknown whether the effects of training will last over time. Last, there might have been a learning effect in this study since the drives were all presented in the same order (to prevent drivers from becoming over sensitized to extreme events) and the event happened in the same location in the drive. Due to the nature of repeated exposure, after experiencing the first drive, participants may have been able to anticipate what would happen in the following drives. However, the models are examined separately for each drive to account for this effect. Future research could consider randomization to avoid this issue.

5.2. Conclusions

A driving simulator experiment was conducted to assess the effectiveness of training and in-vehicle warning messages in improving drivers' response behavior to vehicle cyberattacks. Most drivers did respond to the cyberattacks in a way that was safe and appropriate, e.g., by slowing down, pulling over, or performing cautionary behaviors. The results suggest that drivers' response behavior was moderately affected by the training programs and the warning messages, but only in specific cyberattack events. This research is among the first attempts to incorporate training and warning systems into the human-system loop when studying vehicle cybersecurity. This paper offers automobile manufacturers and cybersecurity experts a new direction and possibly more feasible solutions to potentially alleviate the safety risks caused by vehicle cyberattacks by sharing the responsibility between technological mitigations and human drivers.

Funding details

This project was supported by the National Science Foundation under grant number 1755795. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors/PI and do not necessarily reflect the views of the National Science Foundation.

CRediT authorship contribution statement

Meng Wang: Data curation, Formal analysis, Methodology, Writing – original draft, Writing – review & editing. **Jah'inaya Parker:** Data curation, Investigation, Writing – review & editing. **Fangda Zhang:** Conceptualization, Methodology, Software, Writing – original draft, Writing – review & editing. **Shannon C. Roberts:** Conceptualization, Funding acquisition, Project administration, Resources, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

The authors would like to thank Intisar Becic, the University of Massachusetts Amherst Writing Center, and members of the Cognitive Systems Laboratory at the University of Wisconsin Madison for proofreading the manuscript.

References

Abawajy, J., Kelarev, A., 2012. A multi-tier ensemble construction of classifiers for phishing email detection and filtering. In: Cyberspace Safety and Security: 4th International Symposium, CSS 2012, pp. 48–56.

Akhawe, D., Felt, A.P., 2013. Alice in warningland: a large-scale field study of browser security warning effectiveness. In: Proceedings of the 22nd USENIX Security Symposium, pp. 257–272.

Akwahe, D., Felt, A.P., 2013. Alice in Warningland: A large-scale field study of browser security warning effectiveness. USENIX Security Symposium 13, 257–272.

Aliebrahimi, S., Miller, E.E., 2023. Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles. Transport. Res. F: Traffic Psychol. Behav. 96, 82–91. https://doi.org/10.1016/j.trf.2023.06.010.

Aziz, T., Horiguchi, Y., Sawaragi, T., 2013. An empirical investigation of the development of driver's mental model of a lane departure warning system while driving. IFAC Proceedings Volumes 46 (15), 461–468.

Birrell, S.A., Young, M.S., 2013. Smart driving assistance systems: designing and evaluating ecological and conventional displays. In: Regan, M.A., Lee, J.D., Victor, T. W. (Eds.), Driver Distraction and Inattention: Advances in Research and Countermeasures2. Ashgate, pp. 373–388.

Brooke, J., 1996. SUS: A quick and dirty usability scale. In: Jordan, P.W., Thomas, B., Weerdmeester, B.A., McClelland, I.L. (Eds.), Usability Evaluation in Industry. Taylor & Francis.

Carroll, J.M., Olson, J.R., 1987. Mental models in human-computer interaction. research issues about what the user of software knows. Issues about What the User of Software Knows. Workshop on Software Human Factors: Users' Mental Models.

Casutt, G., Theill, N., Martin, M., Keller, M., Jancke, L., 2014. The drive-wise project: Driving simulator training increases real driving performance in healthy older drivers. Front. Aging Neurosci. 6 (85), 1–14. https://doi.org/10.3389/fnagi.2014.00085.

Chen, Q., Romanowich, P., Castillo, J., Roy, K.C., Chavez, G., Xu, S., 2021. ExHPD: exploiting human, physical, and driving behaviors to detect vehicle cyber attacks. IEEE Internet Things J. 8 (18), 14355–14371. https://doi.org/10.1109/JIOT.2021.3069951.

Classen, S., Winter, S.M., Velozo, C.A., Bedard, M., Lanford, D.N., Brumback, B., Lutz, B. J., 2010. Item development and validity testing for a self-and proxy report: The Safe Driving Behavior Measure. Am. J. Occup. Ther. 64 (2), 296–305.

Cone, B.D., Irvine, C.E., Thompson, M.F., Nguyen, T.D., 2007. A video game for cyber security training and awareness. Comput. Secur. 26 (1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005.

Cranor, L.F., 2008. A framework for reasoning about the human in the loop. In: Proceedings of the 1st Conference on Usability, Psychology, and Security, pp. 1–15.

Davis, F.D., Bagozzi, R.P., Warshaw, P.R., 1989. User acceptance of computer technology: a comparison of two theoretical models. Manag. Sci. 35 (8), 982–1003. http://www.jstor.org/stable/2632151.

Dijksterhuis, C., Stuiver, A., Mulder, B., Brookhuis, K.A., de Waard, D., 2012. An adaptive driver support system: user experiences and driving performance in a simulator. Hum. Factors J. Hum. Factors Ergon. Soc. 54 (5), 772–785. http://hfs.sagepub.com/content/54/5/772.abstract.

Donmez, B., Boyle, L.N., Lee, J.D., 2007. Safety implications of providing real-time feedback to distracted drivers. Accid. Anal. Prev. 39 (3), 581–590. http://www.sciencedirect.com/science/article/B6V5S-4MBT279-1/2/c0ccb26c41271144ee36d468cac2abf8.

Dorn, L., Barker, D., 2005. The effects of driver training on simulated driving performance. Accid. Anal. Prev. 37 (1), 63–69.

Duffy, V.G., 2003. Effects of training and experience on perception of hazard and risk. Ergonomics 46, 114–125.

Duncan, J., Williams, P., Brown, I., 1991. Components of driving skill: experience does not mean expertise. Ergonomics 34 (7), 919–937. https://doi.org/10.1080/00140139108964835.

Eiza, M.H., Ni, Q., 2017. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. IEEE Veh. Technol. Mag. 12 (2), 45–51.

Endsley, M.R., 1995a. Measurement of situation awareness in dynamic systems. Hum. Factors J. Hum. Factors Ergon. Soc. 37 (1), 65–84. https://doi.org/10.1518/001872095779049499.

Endsley, M.R., 1995b. Toward a theory of situation awareness in dynamic systems. Hum. Factors J. Hum. Factors Ergon. Soc. 37 (1), 32–64. http://hfs.sagepub.com/content/37/1/32.abstract.

Endsley, M.R., 2015. Situation awareness misconceptions and misunderstandings. J. Cogn. Eng. Decis. Making 9 (1), 4–32.

Endsley, M.R., Connors, E.S., 2008. Situation awareness: State of the art. In: 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–4.

FBI. 2016. *Motor Vehicles Increasing Vulnerable to Remote Exploits*. https://www.ic3.gov/media/2016/160317.aspx.

Feinauer, S., Schuller, L., Groh, I., Huestegge, L., Petzoldt, T., 2022. The potential of gamification for user education in partial and conditional driving automation: A driving simulator study. Transport. Res. F: Traffic Psychol. Behav. 90, 252–268. https://doi.org/10.1016/j.trf.2022.08.009.

Frese, M., Altmann, A., 1989. The treatment of errors in learning and training. Devel. Skills Inf. Technol. 65–85.
Garcia, J., Feng, Y., Shen, J., Almanee, S., Xia, Y., Chen, A.Q.A., 2020. A comprehensive study of autonomous vehicle bugs. In: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, p. 385396.
Garcia, F.D., Oswald, D., Kasper, T., Pavlides, P., 2016. Lock it and still lose it – On the (in)security of automotive remote keyless entry systems. USENIX Security Symposium 53.
Gemonet, E., Bougard, C., Masfrand, S., Honnet, V., Mestre, D.R., 2021. Car drivers coping with hazardous events in real versus simulated situations: Declarative, behavioral and physiological data used to assess drivers' feeling of presence. PLoS One 16 (2).
Greenberg, A., 2015. Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired. Co*M. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
Hoyle, R.H., Stephenson, M.T., Palmgreen, P., Lorch, E.P., Donohew, R.L., 2002. Reliability and validity of a brief measure of sensation seeking. Pers. Individ. Differ. 32 (3), 401–414. http://www.sciencedirect.com/science/article/pii/S0191886901000320.
Jedrzejczyk, L., Price, B. A., Bandara, A. K., Nuseibeh, B. 2010. On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*. https://doi.org/10.1145/1837110.1837129.
Khan, S.K., Shiwakoti, N., Stasinopoulos, P., Chen, Y., 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid. Anal. Prev. 105837.
Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Snachám, H., Savage, S., 2010. Experimental security analysis of a modern automobile. Proc. IEEE Symp. Secur. Privacy 447–462. https://doi.org/10.1109/SP.2010.34.
Krampell, M., Solís-Marcos, I., Hjälmdahl, M., 2020. Driving automation state-of-mind: Using training to instigate rapid mental model development. Appl. Ergon. 83 (August 2018) https://doi.org/10.1016/j.apergo.2019.102986.
Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., Hong, J., 2010. Teaching Johnny not to fall for phish. ACM Trans. Internet Technol. 10 (2), 1–31. https://doi.org/10.1145/1754393.1754396.
Lee, J.D., Gore, B.F., Campbell, J.L., 1999. Display alternatives for in-vehicle warning and sign information: message style, location, and modality. Transp. Hum. Factors 1 (4), 347–375. https://doi.org/10.1207/sthf0104_6.
Lesch, M.F., Horrey, W.J., Wogalter, M.S., Powell, W.R., 2011. Age-related differences in warning symbol comprehension and training effectiveness: effects of familiarity, complexity, and comprehensibility. Ergonomics 54 (10), 879–890.
Lesch, M.F., Powell, W.R., Horrey, W.J., Wogalter, M.S., 2013. The use of contextual cues to improve warning symbol comprehension: making the connection for older adults. Ergonomics 56 (8), 1264–1279.
Maltz, M., Shinar, D., 2004. Imperfect in-vehicle collision avoidance warning systems can aid drivers. Hum. Factors: J. Hum. Factors Ergon. Soc. 46 (2), 357–366. http://hfs.sagepub.com/content/46/2/357.abstract.
McCarthy, C., Harnett, K., Carter, A., 2014. Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach. National Highway Traffic Safety Administration.
Ouimet, M.C., Pradhan, A.K., Simons-Morton, B.G., Divekar, G., Mehranian, H., Fisher, D.L., 2013. The effect of male teenage passengers on male teenage drivers: Findings from a driving simulator study. Accid. Anal. Prev. 58, 132–139. https://doi.org/10.1016/j.aap.2013.04.024.
Parker, J., Zhang, F., Wang, M., Roberts, S.C., 2022. How do drivers respond to vehicle cyberattacks? A driving simulator study. Human Factors and Ergonomics Society Annual Meeting Proceedings 737.
Petit, J., Shladover, S.E., 2014. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 1–11.
Pfleeger, S.L., Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. Comput. Secur. 31 (4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010.
Pollard, J., Fisher, D., Guglielmi, J., Mattson, A., Young, J., Lucibello, G. 2017. Driver ability to cope with unintended acceleration by shifting gears in a simulator experiment. *Transportation Research Board 96th Annual Meeting*.
Ranney, T., 2011. Psychological fidelity: The perception of risk. In: Fisher, D.L., Rizzo, M., Caird, J., Lee, J.D. (Eds.), Handbook of Driving Simulation for Engineering, Medicine, and Psychology. Routledge.
Reimer, B., D'Ambrosio, L.A., Gilbert, J., Coughlin, J.F., Biederman, J., Surman, C., Fried, R., Aleardi, M., 2005. Behavior differences in drivers with attention deficit hyperactivity disorder: The driving behavior questionnaire. Accid. Anal. Prev. 37 (6), 996–1004. https://doi.org/10.1016/j.aap.2005.05.002.
Roberts, S.C., Zhang, F., Fisher, D., Vaca, F.E., 2021. The effect of hazard awareness training on teen drivers of varying socioeconomic status. Traffic Inj. Prev. https://doi.org/10.1080/15389588.2021.1940984.
Salas, E., Stout, R. J., Cannon-Bowers, J. A. 1994. The role of shared mental models in developing shared situational awareness. In: *Situational awareness in complex systems* (pp. 297–304).
Simons-Morton, B.G., Zhang, Z., Jackson, J.C., Albert, P.S., 2012. Do elevated gravitational-force events while driving predict crashes and near crashes? Am. J. Epidemiol. 175 (10), 1075–1079. https://doi.org/10.1093/aje/kwr440.
Soliman, A.M., Mathna, E.K., 2009. Metacognitive strategy training improves driving situation awareness. Soc. Behav. Personal. Int. J. 37 (9), 1161–1170.
Unni, A., Ihme, K., Jipp, M., Rieger, J.W., 2017. Assessing the driver's current level of working memory load with high density functional near-infrared spectroscopy: a realistic driving simulator study. Front. Hum. Neurosci. 11, 167.
Unverricht, J., Samuel, S., Yamani, Y., 2018. Latent hazard anticipation in young drivers: review and meta-analysis of training studies. Transp. Res. Rec. 2672 (33), 11–19. https://doi.org/10.1177/0361198118768530.
Wan, J., Wu, C., Zhang, Y., 2016. Effects of lead time of verbal collision warning messages on driving behavior in connected vehicle settings. J. Saf. Res. 58, 89–98.
Wickens, C.D., Hollands, J.G., Banbury, S., Parasuraman, R., 2013. Engineering Psychology and Human Performance, 4th ed. Pearson Education Limited.
Wickens, C. D. 1992. Virtual reality and education. In *1992 IEEE International Conference on Systems, Man, and Cybernetics*, 842–847.
Wickens, C.D., Carswell, 2012. Information processing. In: Salvendy, G. (Ed.), Handbook of Human Factors and Ergonomics. John Wiley & Sons Inc.
Wolf, M., Weimerskirch, A., Wollinger, T., 2007. State of the art: embedding security in vehicles. EURASIP J. Embed. Syst. 2007, 1–16. https://doi.org/10.1155/2007/74706.
Zhang, F., Petit, J., Roberts, S.C., 2019. A simulator study on drivers' response and perception towards vehicle cyberattacks. Hum. Fact. Ergon. Soc. Annu. Meet. Proc. 63, 1498–1502.
Zhang, F., Wang, M., Parker, J., Roberts, S.C., 2023. The effect of driving style on responses to unexpected vehicle cyberattacks. Safety 9 (1), 5. https://doi.org/10.3390/safety9010005.