Today's vehicles are the ultimate electronic devices, and tempting targets for cyberattack. What are you doing to protect your shop's property and data, as well as that of your customers?
Cybersecurity has become everyone’s business. Driven by software, vehicles are being increasingly networked to each other via Intelligent Transportation Systems (ITSs) connected to numerous computing clouds and the Internet of Things (IoT). While we’re headed toward smart, efficient and automated mobility, it’s not all peaches and cream.
“Cybersecurity is a complex, evolving target,” explained Bruce Schneir, a renowned security technologist and Chief Technology Officer for IBM Security’s cyber resiliency platform. “As transportation and its connected devices come under pervasive software control, they are more vulnerable to all the previous types of cyberattacks that we’ve seen before in other industries, as well as new ones emerging today specific to the IoT.

“The IoT is more sophisticated than every previous computing technology,” he insisted. “Thousands of diverse devices, operating systems and protocols are connected to the IoT every day, vastly increasing the cyberattack landscape. Worse, up to 80% of all current IoT-connected devices, including automobiles, lack the security measures necessary to protect us. Not only must security be in place across the whole industry spectrum—on the devices, clouds and the IoT—every industry layer, from automakers to service and repair facilities, must be actively involved.”

So what’s a shop to do? Let’s start by getting an understanding of how cybersecurity is evolving first at the global level, then work our way through the complementary security measures automakers, toolmakers and shops can implement.

Industry stakeholders must demolish their proprietary silos and learn from and collaborate with one another. Security must be in place across the whole spectrum—on the devices, the cloud and the IoT.

“Because data can flow many ways, industry standards and stakeholder collaboration are essential,” stated Jack Pokrzywa, Director for Cybersecurity Standards at the Society of Automotive Engineers (SAE). “The SAE, the International Organization for Standardization (ISO), aftermarket associations, governments, Congress and regulators are in constant discussions pertaining to data and functional security. They are leaning their proprietary silos, determining security gaps, jointly defining standards, synchronizing strategies and implementing cyber countermeasures to minimize the exposure and vulnerabilities of vehicles.”

Of note, the SAE Vehicle Cybersecurity Systems Engineering Committee recently published the world’s first automotive security standard and guidebook, titled The J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems. Said Pokrzywa: “J3061 describes a risk-based, process-driven approach to address the cybersecurity threats the automotive environment is experiencing and to serve as a foundation of best practices for research conducted by several SAE committees in related discipline areas.”

In particular, access to vehicle communication networks is becoming more cloud- and IoT-based, paving the way

---

**STANDARDS BUILD THE BASE**

The Society of Automotive Engineers (SAE) and the International Organization for Standardization (ISO) recently approved the Partner Standards Development Organization, which created a Joint Working Group (JWG) tasked with developing harmonized joint SAE-ISO standards. Representation spans 10 ISO nations and 11 SAE subject matter experts. To date, the JWG has already developed processes, procedures and rules the template for all joint work projects, which currently include harmonizing standards for cybersecurity, vehicle data access, vehicle-to-infrastructure interoperability and vehicle automation levels.

Project participants include 10 automakers, 11 Tier One suppliers, aftermarket organizations and dozens of cybersecurity firms, consultants and other suppliers, who are now engaged in the technical work of developing standards.
for more secure, modern and robust vehicle communication interfaces (more commonly called gateway modules) to be installed in vehicles. The leading example is the ISO’s proposed Extended Vehicle (ExVe) concept and related hardware. As currently written, access to vehicle data, software and other information would become cloud-based on servers owned and operated by individual automakers, each of whom would control who had access, and to what degree. In other words, access by different users on the IoT would be secured, tiered, limited and authorized by the automaker.

Aftermarket representatives at SAE and ISO appreciate the improved security ExVe offers, but want shared automaker-aftermarket control of access, vetting of users and degree of access. For this reason, the Equipment and Tool Institute (ETI), the Auto Care Association and others are engaged in discussions to try to reach a resolution that improves security, keeps a level competitive field and best serves the public interest.

“If the automakers are able to limit connectivity, then legitimate access for everything from diagnostics, prognostics, fleet management, insurance monitors, vehicle owner convenience features and consumer advocate researchers and watchdogs will be provided only by the vehicle manufacturer,” suggested Greg Potter, ETI Executive Manager and member of SAE and ISO. “This will impede fair competition in the marketplace, and put the public interest at risk.

“Instead, we’d like to see open standards that follow the ‘Bounded, Secure, Managed, Domain (BSMD)’ approach, as is being developed for vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications for the Intelligent Transport Systems (ITS) model,” Potter added. “This communications structure can work for many use-cases besides ITS. By sharing in this ITS-based hardware and software, vehicle manufacturers and the aftermarket can both save time and money on a workable solution.”

**Service & Repair Changes**

“Service and repair shop owners and technicians also need to know what is going to change and when it will impact them, especially in the short term,” emphasized Bob Gruszcznski, the OBD Specialist for Volkswagen Group of America and a member of SAE and ISO. “We not only want to ensure technicians have the same or better access to everything from diagnostics, prognostics, fleet management, insurance monitors, vehicle owner convenience features and consumer advocate researchers and watchdogs will be provided only by the vehicle manufacturer,” suggested Greg Potter, ETI Executive Manager and member of SAE and ISO. “This will impede fair competition in the marketplace, and put the public interest at risk.

“Instead, we’d like to see open standards that follow the ‘Bounded, Secure, Managed, Domain (BSMD)’ approach, as is being developed for vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications for the Intelligent Transport Systems (ITS) model,” Potter added. “This communications structure can work for many use-cases besides ITS. By sharing in this ITS-based hardware and software, vehicle manufacturers and the aftermarket can both save time and money on a workable solution.”

You can increase repair orders

**Quick Check:**

- Inspection results in under 2 minutes
- Drive alignment sales, the highest profit margin service
- Digital and printed results enhance customer loyalty

Circle #12
The current J1962 DLC is 30 years old and needs to be replaced. Auto-
makers do not own the underdash DLC that we connect scan tools, re-
programming J2534 boxes, dongles and other devices to. Rather, it’s jointly owned by the U.S. En-
vironmental Protection Agency (EPA) and California Air Resources Board
(CARB), which mandated the minimum functionality automakers must 
enable. They have relied on the SAE to set the necessary standards and 
procedures for the seven original communication protocols, vehicle 
connectors and on-board diagnostic 
data required.

As vehicle technology has ad-
vanced over time, advanced function-
ality has been added out of necessity 
to diagnose and service vehicles. 
“The old J1962 DLC is not capable 
of meeting the demands of modern 
automobiles,” Gruszcznski noted. 
“Examples include more advanced 
communication protocols, J1954 
programming and other enhanced 
diagnostics, which represent a large 
part of the diagnostics and service 
we all perform in service and repair 
facilities today. Although governed 
by SAE standards, these are not re-
quired by the EPA or CARB.

“New advanced replacement DLCs 
developed by OEMs do meet mod-
ern demands,” he added. “They allow 
multiple users access to vehicle com-
munication networks and data that is 
tiered, limited to need-to-know, au-
thorized and able to be processed fast 
enough to be safe in real time. The 
industry is waiting on the EPA and 
CARB to accept modern realities and 
let standards help service and repair 
keep current with technology and ca-
pable of deterring threats.”

The rise of cybersecurity attacks is 
everyone’s problem and may spark 
the change needed. It’s important 
to understand that legislated OBD II 
diagnostics are “read-only” files. 
They pose no cyberthreat, so vehicles 
cannot be hurt. However, enhanced 
diagnostics files are “writeable” and 
thus far more interactive. Data and 
settings can be changed, which puts

The vehicle at risk if unsecured. Re-
cently, Congress, the U.S. Dept. of 
Transportation and NHTSA asked 
the SAE to help integrate an elevated
level of cybersecurity.

“Service and repair facilities and 
technicians need to know that SAE 
has just developed a new standard—
The J3138 Guidance for Securing the 
Data Link Connector,” Gruszcznski 
explained. “The new standard is in-
tended to provide guidance to OEMs 
for securing DLCs from the cyberse-
curity risks posed by the existence of 
this connector. The document con-
siders three different vehicle archi-
tectures in play between the DLC 
and diagnostic functions: One type 
uses a master gateway, another relies 
on less sophisticated security mea-
sures and the last is a hybrid of the 
two—some of the vehicle communi-
cation topology uses a gateway, while 
the rest is individually oriented.

“The document’s intent is to put 
vehicles into a safe mode of opera-
tion to secure them from a successful 
cyberattack in real time that could 
be harmful to people on the road,”
noted. “We need to be more than just aware of cybersecurity; we must prepare on behalf of our customers—the OEMs who build vehicles, as well as the service and repair professionals who maintain and fix them. To keep pace, cybersecurity will continue be an ongoing focus for ETI. Securing tools, equipment and other services that connect to automobiles is an essential step in the evolution of cybersecurity.”

Two recent successful cyberattacks come to mind that demonstrate terrible vs. excellent cybersecurity.

Safeguard Your Arsenal
“Emerging intelligent transportation systems—which tools, equipment and connected information services will be part of—require high-speed, real-time data analysis and processing to deliver meaningful, timely and safe results,” ETI’s Greg Potter shared. “That’s driving us to the cloud and the IoT. On a macro level, avoiding data paralysis is another challenge. Cloud computing, the IoT, connected vehicles, advanced driver assistance systems (ADAS), automated driving and other emerging technologies all create enormous volumes of data, which can create congestion and latency issues.”

“With the advent of telematics, connected vehicles, automated driving, intelligent transportation systems and the IoT, this segment needs complete solutions now,” shared Mohan Sethi, Business Development Manager for MAHLE Service Solutions. “On a micro level, every connected electronic diagnostic tool, piece of equipment, device and service is prone to attack and capable of easily being hacked. For example, if a J2534 tool is infected with malware, then every vehicle and device that J-box is then connected to is at risk, until the attack is remedied.”

“Think of the automobile as the ultimate electronic device today,” Potter advised Gruszcznski. “Automakers would be responsible to ensure vehicles are in a safe state before allowing the steering rack to be moved, brakes bled, etc. For example, a request to bleed the brakes would require confirmation from a secure vehicle system or service professional with a scan tool that PRNDL is in Park, the parking brake is set, the door and hood switch are both open—in short, that the vehicle is at a standstill and not moving, whether at 50 or 5 mph. The new J3138 standard is now complete and is under ballot.”
The first is Equifax, a financial credit rating company that was successfully hacked on May 13, 2017, and exposed the personal identity information of hundreds of millions of its customers. While the breach was a result of a vulnerability in an Apache software program that Equifax used, Apache had fixed the vulnerability on Mar. 6—more than two months before the cyberattack—with a security patch that it and the Dept. of Homeland Security urged Equifax to install immediately. Yet Equifax didn’t get to install the security patch until July 29—more than two full months after the attack.

At the opposite end of the spectrum, consider Bosch. The major Tier 1 supplier and ETI member first began selling its Drivelog Connector OBD II dongle and associated Drivelog Connect smartphone app in early 2016. The underdash dongle accesses vehicle health data over the on-board Controller Area Network (CAN) bus, while the app enables vehicle owners to connect to the dongle remotely and review that data. Both products were simultaneously hacked in April 2017. The most serious threat, exploitable remotely through either product, was that the engine could be remotely shut off while the vehicle was moving, whether at low or high speed. What sets Bosch apart is how it reacted.

In conjunction with security consultant Argus Cyber Security, Bosch immediately safeguarded vehicle occupants by ceasing all dongle and app connections and implementing a mandatory, two-step verification procedure customers had to complete to reactivate the products. At the same time, Bosch also prevented any further breaches by releasing application software and dongle firmware updates that prevented similar attacks from placing malicious code onto the CAN bus. Since the attacks, Bosch has rolled out additional preventive cybersecurity measures it developed to further limit the penetration by unwanted CAN messages.

Service and repair businesses do not have to sit back and live with the consequences of cyberattacks. Awareness can help separate the wheat from the chaff by verifying, rather than assuming or blindly accepting, that the companies you do business with have adequate security in place. To do this, query the firms in this segment that your shop relies on about their cyberattack preparedness. A plan similar to Bosch’s would be awesome, but if a vendor can’t (or won’t) disclose to your satisfaction the type of cyber countermeasures it utilizes, odds are adequate security is lacking. Better to know that upfront than be potentially blindsided later. Then consider two questions:

- Do you really want unsecure vendors, products and services connecting to your primary shop network?
- Can you afford the liability and financial risk of not being cybersecure?

**The Last Line of Cyber Defense**

“It took OEMs a long time to take cybersecurity seriously, let alone put substantial resources behind tackling it,” shared Dr. Anuja Sonalker, the CEO of STEER Tech and Vice Chair of the SAE Vehicle Cybersecurity Systems Engineering Committee. “Consequently, other automotive sectors soft-pedaled on security. That all changed in 2015, a breakout year, if you will. The first public demonstrations of remote hacks of vehicles occurred, following private ones the year before. The first cybersecurity-associated NHTSA recall also occurred, resulting
in $1.4 billion in recall expenditures and another $105 million in fines. Later in the year, the first cybersecurity action against a Tier 1 supplier was initiated by NHTSA and several related class suits were launched, none of which has yet to be completed. These milestones woke up the rest of the industry to the realization that not having adequate cybersecurity in place has substantial costs, too."

Since 2015, the Automotive Service Association (ASA) has been actively engaged in developing guidelines and policies to help its member service and repair shops become more cybersecure. It still is. ASA’s ongoing dialogue with its members spans recruiting new talent, hack-proofing service and repair shops, safeguarding connected tools and equipment, securely servicing customers’ vehicles, best practices and evolving cybersecurity solutions to detect and respond to cyberthreats.

“As an industry, we need to shift recruitment, student education and aftermarket training from an Industrial Age mindset to a Technological Age mindset,” urged Jeff Peevy, President of the ASA’s Automotive Management Institute. “We must forsake archaic practices and strive collectively to be caretakers of our professions. These days, cybersecurity must be built into that mindset.”

“IT software programming skills are just the tip of the iceberg,” Volkswagon Group’s Gruszcynski specified. “But what we really need to attract is cybersecurity expertise—the aptitude, skillset and understanding of security protocols and procedures necessary to offset the vulnerabilities that piggyback the introduction of new technologies. Automobile communications are on the cusp of major change. To remain competitive and secure, service and repair facilities will need to begin employing IT-savvy technicians or specialists.”

“Vehicles, systems, connected networks and other resources in shops must be compartmentalized, with different security requirements and encryption measures capable of preventing or allowing access to vehicle data, including what level of access,” STEER Tech’s Dr. Sonalker cautioned. “Here are four simple and inexpensive measures shops can take to begin locking down:

• When purchasing computer equipment, buy new high-quality equipment from reputable sources. Buying cheap or used is a quick way to get malware or embedded spy chips.

• Hire a knowledgeable IT professional—about $500 should cover the consult—to help you segregate primary internal networks and connected resources.

• Consider buying a network security scanner, such as the Nessus remote device. Scanners monitor a computer and raise an alert if they discover any vulnerability that malicious hackers could use to gain access to any computer you have connected to a network.

• Use firewalls to create a shop demilitarized zone (DMZ), which separates the public (and potentially malicious actors) from secured and trusted internal network(s) with sensitive data.”
“Ensure the latest software and security patches are immediately installed on the devices you use and other resources you connect to,” advised Craig Smith, Research Director of Transportation Security at Rapid7 Inc. “This is absolutely critical when it comes to safety within a vehicle and security of the shop. But that best practice goes only partway. Shops should also consider regular and frequent penetration testing of their primary locked-down network to ensure the safety and security of the resources and services connected to it. For instance, Rapid7’s Metasploit Security Kit enables professionals and researchers to use a single tool to quickly conduct penetration testing of both hardware and software for vulnerabilities and attacks.”

“At no time in the history of the automotive industry has technological change been so dramatic, so imaginative, so exciting, so fast and so in need of your engagement,” cautioned Mahbubul Alam, Chief Technology Officer of Movimento Group, a Delphi company. “New types of data you likely haven’t heard of yet will be communicated over-the-air to vehicles within the next five years. Independent shop owners and service repair professionals need to adopt a new mentality that vehicle cybersecurity is never completely done. It must be built-in from the beginning, and be continually maintained and upgraded thereafter.”

Make no mistake, cybersecurity has indeed become a necessary part of everyone’s business. But the responsibility for making sure it’s implemented to the last mile rests with you. The question is: Are you actually prepared and willing to do the work to keep your shop and your customers safe and secure?

Recruiting & Retaining Today’s Techs

continued from page 25

We always have several job posts running, so interviewing one or two candidates per week is not uncommon and enables us to keep watch of the current “puddle.” Last fall, we interviewed a candidate who ran a quick-lube establishment. He had no diagnostic skills, lacked a complete set of tools and didn’t have any certifications. He told us his minimum salary requirement would be to match his current annual income of $82,800. He later e-mailed me asking what our dental, vision, disability and 401k plans entailed. Don’t get me wrong: I think everyone deserves a decent paycheck and all the benefits in the world. I think I do! Unfortunately for this candidate, we had already calculated our budget for a low-to-midlevel technician, and it was less than what he required. We politely informed him to work on his skillset and perhaps we might reconsider him later.

It took some time, but we ended up hiring a midlevel technician with an excellent attitude, a near-complete set of tools and experience that not only matched our budget, but enabled us to offer him more money than his previous facility and a health insurance package on top of that. With the added leadership qualities of our management team (transparency, documentation, genuine support), we love him, and he loves us back. He asks my service writer, a former technician, a ton of questions throughout the day, and the writer genuinely helps. In turn, the new tech trusts the writer and provides us with excellent diagnostic and inspection information. Each time the tech completes a successful repair he has performed for the first time (an electrical repair, for instance), the whole team congratulates him and thanks him for his efforts. We reward him with gift cards and goodies to take home to his wife, plus flexibly grant him time off. So, following David Rogers’ advice, we’re using proper recruiting strategies by staying within our numbers and retaining good technicians by creating an internal culture that ensures the staff feels needed, valued and successful. The tech pool is smaller, but it’s not empty!

It Ain’t Easy!

How to best recruit and retain techs? It’ll never happen until you, the boss, become a true leader, an advocate for the team who has a solid handle on the numbers and isn’t letting ego get in the way of success. Look in the mirror. Is your facility super grungy? Are you making promises you don’t keep? Are you abandoning the new hires? Are you clearly training the staff according to your expectations?

This industry is hard for all of us. It’s demanding. Recognize this with your team every day. Know their feet and backs hurt. Know they need to be paid more time to diagnose tricky cases, or fix stuff that isn’t their fault. Know they need to eat and hydrate more, and need a day off once in a while.

“I can never be the biggest shop,” David Rogers told me. “I can never be the highest paying shop because I don’t have the extra two million dollars in cash a year to hand everybody. But what I can do is be the most real and the most trustworthy guy that you have ever met and worked with and that is my goal every day when I get out of bed. I want people to know it’s real and I want them to see me eat my own crow and correct myself and bring my problems to the team just like I’m asking them to do.”

Stay committed to your numbers and to the qualities that make a good leader, and the next time a fellow shop owner grumbles about the lack of good techs, you might find yourself asking him about his stats and leadership strategies rather than grumbling along with him.