Cyber readiness: are auto companies prepared to counter the risk of an attack?

pwc

www.pwc.com/automotive

The automotive industry is facing an inflection point: As internet connectivity becomes commonplace, it increases the risk that privacy – and even safety – will be compromised. While automakers have stepped up their game to meet consumer demand for connected cars, some are inadequately addressing the cyber risks inherent in mobile connectivity.

In 2015, we got a glimpse at what is at stake, when two security researchers hijacked a vehicle over the internet. They were able to turn the steering wheel, briefly disable the brakes, and shut off the engine. The implications of this exercise were clear and troubling at the time. Now, three years later, with many more cars internet-enabled, the risk of hijacking has exploded. And the trend is likely to continue as consumers have become accustomed to the convenience of connectivity. However, every new convenience adds risk, and current security protections generally fall short of countering that risk.

1. Andy Greenberg, Wired, "The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse," Aug. 1, …" https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

The inherent cyber risks of connected cars

Citing the growing threat of cyberattacks shortly after two security researchers remotely hacked into the software of a vehicle in 2015, the U.S. Department of Homeland Security (DHS) invested almost $4 million in two research projects to assess the security of connected vehicles.[2] In 2016, researchers from a security company identified a weakness in a vehicle entertainment system that could lead to a ransomware attack.[3] Then, last summer, the DHS National Cybersecurity and Communications Integration Center and Industrial Control Systems Cyber Emergency Response Team (ICS-Cert) issued an advisory notifying several automobile makers of new research that identified a weakness in on-board telematics control modules that could lead to a denial-of-service attack.[4]

Intrusion through the internet

While consumer demand may be driving new technology adoption in vehicles, security protections may not address all the cyber risks. Nearly every car for sale today has a telematics unit and other components that provide a connection to the outside world. Connected car components make it possible to remotely attack infotainment, diagnostic functions, or even core features like the engine control unit (ECU). New cars have been equipped to provide real-time status information and possess the ability to control aspects of the car remotely. These features rely on Bluetooth and Wi-Fi and cellular radio signals to communicate, while their underlying computers are often based on platforms with both software and hardware vulnerabilities. They connect with the infotainment systems on car dashboards, which closely interact with travelers in the car through their mobile phone devices. As a connected device, a vehicle can be subverted if its security is compromised; anything that the vehicle is capable of can be controlled by the attacker—to the point of endangering life and limb. Even customers who do not subscribe to remote connectivity features are at risk. Cars can also become a source of risk to the enterprise because the two are connected to one another and an intrusion via telematics can lead to a breach in enterprise defenses.

Although there are no known malicious acts that have actually exploited connected vehicles, it is likely to be only a matter of time. Security researchers have shown that key areas of the vehicle can be hacked. As manufacturers connect additional features and technologies, vulnerabilities will grow. And the move toward autonomous vehicles is only likely to exacerbate the threat.

Compromising consumer privacy

Another growing concern with connected cars is consumer privacy. A great deal of data can be captured through in-car networks (e.g., geographic location, speed, and even whether the style of driving is aggressive) and, as cars become even more connected, the amount of data captured will increase. While the selling of car-related data is still in its infancy, this is an area that is set to explode because of the commercial possibilities. Many companies would be interested in obtaining car-related data, most notably, insurance, advertising, and energy firms. And car companies would be glad to have this high margin revenue stream. However, the sale of car-related data poses significant implications for consumer privacy.

"As a connected device, a vehicle can be subverted if its security is compromised; anything that the vehicle is capable of can be controlled by the attacker..."

2. "https://securityledger.com/2015/11/dhs-funding-research-into-secure-updates-for-vehicles/".
3. Paul, The Security Ledger, "Update: DHS Funding Research Into Secure Updates for Vehicles," May 16, 2018 (updated from Nov. 9, 2015); "https://securingtomorrow.mcafee.com/mcafee-labs/defcon-connected-car-security/".
4. Mark Rockwell, FCW, "DHS, vendor warn on automotive cyber flaws," Aug. 3, 2017; "https://fcw.com/articles/2017/08/03/auto-cyber-cert-rockwell.aspx"

Combating connected car risk

While many companies understand the need to address cyber risks, they often classify it as a technology problem rather than a business one, limiting the tools they use to fight cyber risk. And they are dealing with cyber criminals who are increasingly sophisticated and adept at their craft. So automotive companies that continue to rely on reactive security and risk management principles are left with inadequate security protections, exposing them to significant cyber risk and the potential consequences of intrusions.

Quality management

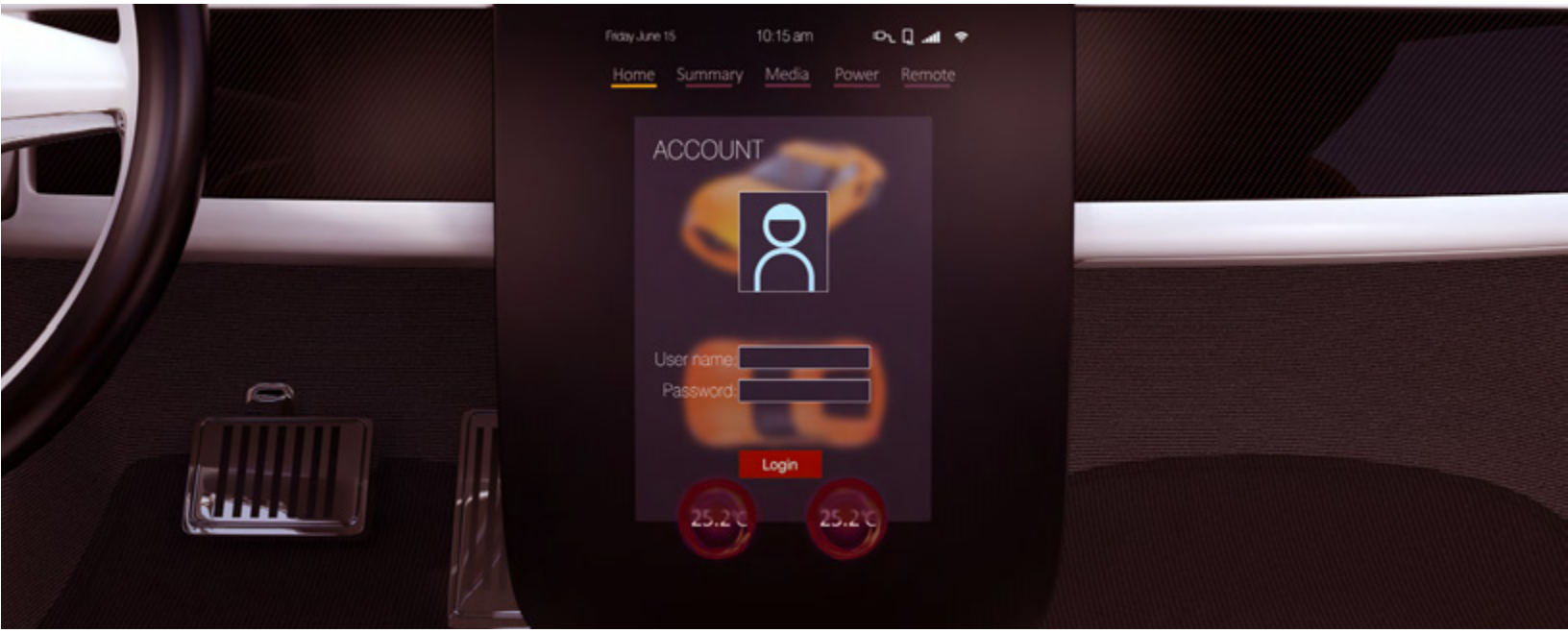
Automotive manufacturers are still in reactive mode, fixing problems that have been identified, rather than getting ahead of the curve. This approach is fraught with issues, including potential liability, expensive recalls, and reputational damage.

Instead, companies need to seek out potential vulnerabilities, fix them, create requirements, and then communicate those requirements to vendors. While some automakers might think that being proactive is beyond their capability, the process is similar to traditional quality management, which identifies and fixes defects. In the cyber world, the vulnerabilities of connected cars are really product defects. Companies can use the quality management systems they already have in place by embedding cybersecurity components into the engineering process and fixing vulnerabilities as they would other product defects.

Cybersecurity integration into design

Security has to be built into cars as an integral part of product design. Unlike traditional IT solutions or cybersecurity enterprise solutions, it is impossible

"In the cyber world, the vulnerabilities of connected cars are really product defects."



to add either security technologies or features after the fact. So vulnerabilities need to be identified and dealt with before they go into production. Since cars typically have a three-to-five-year product development life cycle, one or two testing cycles is insufficient. Early testing will catch the majority of vulnerabilities, but other defects are likely to emerge later in the process. Also, following the identification of a defect, car makers have to retest to ensure it has been remediated and no new vulnerabilities have been introduced. Although adding reiterative security testing may attenuate the overall development cycle, fixing issues early reduces the cost of remediation. In the long run, secure design will limit recalls, reduce liability risk, and help maintain brand reputation.

Cybersecurity integration into supply chain

Supply chain security integration is a critical part of this proactive approach to cybersecurity. The majority of sophisticated components in a connected car come from third party suppliers. But defects post-production will be identified with the brand of the manufacturers, not a supplier. The onus is on car makers to communicate testing results to their vendors, proactively develop security requirements, push these requirements to vendors, and ensure that vendors follow through.

Information sharing

There are no clear standards yet on cybersecurity requirements for the industry, but the Automotive Information Sharing and Analysis Center (Auto-ISAC) released a set of cybersecurity best practices for connected vehicles.[5] The Auto-ISAC serves as a repository of intelligence on cyber threats to help the automotive industry prepare for and respond to vehicle cybersecurity risks. Automotive companies can strengthen their ISAC by being diligent in sharing threat information and analysis. Early this year, the Auto-ISAC signed an agreement with the DHS to collaborate on vehicle cyber threats, which promotes collaboration between the industry and experts in the federal government.

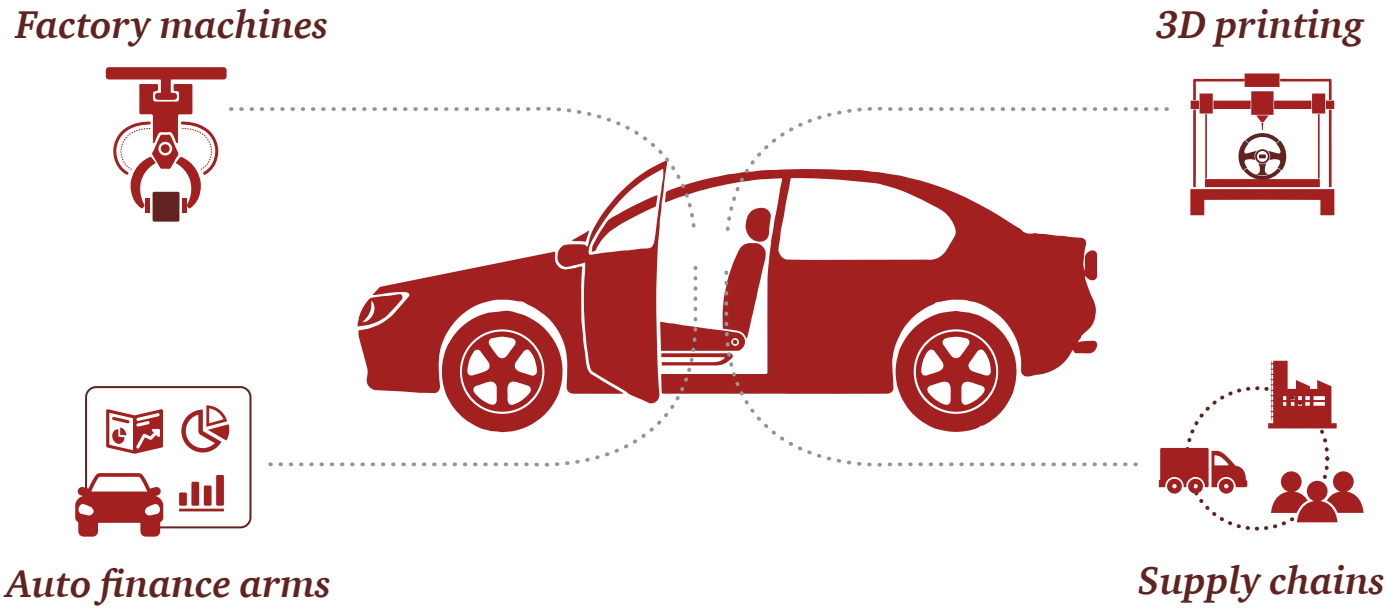
5. Automotive Information Sharing and Analysis Center (Auto-ISAC), Cision PR Newswire, "Auto-ISAC signs cybersecurity agreement with DHS," Jan. 25, 2018; https://www.prnewswire.com/news-releases/auto-isac-signs-cybersecurity-agreement-with-dhs-300588475.html

Cyber risks to the enterprise

Car safety has to be supported by an enterprise-wide program that coordinates cyber defenses across all production platforms, internal operations, and supply chains. A weakness in one area can infect the rest of the enterprise and result in, for example, car failure, factory slowdowns, the hacking of customer data, or the theft of intellectual property. There are several obvious entry points for intruders, including:

1. *Factory machines:* Equipment is often built for 100% uptime and is rarely shut down for patching or upgrading. As with other legacy technologies with inadequate control systems, such machines present risk to the enterprise and its corporate functions, especially when connected to the internet.
2. *3D printing:* A growing part of the prototyping and additive manufacturing processes, 3D printing uses digital files that can be stolen.
3. *Auto finance arms:* These entities collect a great deal of customer data. Data theft can result in financial loss and the tarnishing of an organization's reputation.
4. *Supply chains:* All third parties present some element of risk; smaller vendors, who often lack adequate security controls, present a particular vulnerability. Supply chain risk will increase exponentially as the internet of things (IoT) transforms interactions between OEMs and suppliers through greater transparency and efficiency.

Potential entry points



"Car safety has to be supported by an enterprisewide program…A weakness in one area can infect the rest of the enterprise."

Combating enterprise risk

While many companies understand the need to address cyber risks, they often classify it as a technology problem rather than a business one, limiting the tools they use to fight cyber risk. And they are dealing with cyber criminals who are increasingly sophisticated and adept at their craft. So automotive companies that continue to rely on reactive security and risk management principles are left with inadequate security protections, exposing them to significant cyber risk and the potential consequences of intrusions.

Holistic, layered approach

Cyber resilient companies develop a holistic approach to fighting cyberattacks that includes prevention, detection, and reaction as well as a feedback mechanism. But no solution is foolproof; some attacks will get through prevention measures and others will go undetected. Mature, global automotive organizations should expect hundreds of low-impact attacks and perhaps dozens of more serious attacks every year. Preventing or even slowing down attacks requires a layered approach that combines multiple security controls and established procedures for prevention, detection, and reaction.

First and foremost, manufacturers need to focus on preventing incidents. It invariably costs less to prevent an attack than deal with the subsequent consequences. But once an attack occurs, it is necessary to detect it as quickly as possible in order to isolate the damage. The ability to move decisively and swiftly not just limits losses, but prevents an intruder from temporarily pausing the attack and hiding elsewhere in the enterprise's networks, only to attack at a later date.

Unfortunately, it takes an average of 6-18 months to detect an intrusion, and many companies don't even know they have dormant penetration. So once an intrusion is detected, a company has to mount a vigorous reaction to prevent the intruder from penetrating more deeply into the organization's network and causing widespread harm.

Following are some of the industry's best practices for securing the enterprise against cyber threats:

1. *Get buy-in at the highest levels to build a security culture.* As with any other critical risk, C-level executives and the board of directors need to be engaged in budgeting for security and fostering a security culture throughout the organization. All employees have to share in security awareness and understand their roles and responsibilities in preventing cyber attacks. Any part of the organization can become a victim of intrusion, and a failure in one area can affect the others. Security policy and heightened awareness of cyber risk have to be woven into the fabric of the culture through tone at the top, education, and HR policies.

   A good illustration of how the lack of awareness can impact a company is the continuing success of phishing, a commonly used practice and still effective against unsuspecting personnel. Phishing can yield significant returns, even if just one target takes the bait. An employee who opens an email link containing malware can infect an entire organization.

2. *Prioritize assets and threats.* Since it's too expensive to protect all assets, automotive companies should determine which are their most valuable ones and focus aggressively

"Unfortunately, it takes an average of 6-18 months to detect an intrusion, and many companies don't even know they have dormant penetration."

on protecting them. Companies also need to categorize and prioritize the kinds of threats they are facing, now and in the next few years, as well as the perpetrators most likely to do damage. Some companies use threat intelligence services to help keep track of the latest industry threats, which are then fed back into security operations procedures.

3. *Define and integrate processes.* Clearly defined processes help to reduce the time from incident to detection to response. They should include a matrix that places attacks on a graduated scale of potential impact based on degree of financial/operational/brand exposure, number and type of systems compromised, and a clear plan for notifying internal and external stakeholders. They should also contain sensitivity and analytical capability that can discern false positives driven by external or internal events unrelated to an intrusion.

Different triage procedures come into play for major/minor incidents, including which business units to notify and whether to deploy a crisis-related public relations strategy. The vast majority of incidents tend to be of very low severity. But it is useful to establish regular metrics around these incidents to help identify patterns that can highlight opportunities for improvement, cost savings, and risk reduction.

Leading organizations have a structured, lessons-learned process that allows them time to review and update procedures and tactics: What went well? What didn't? How can efforts be improved? What specific actions need to be taken and by whom? The answers to these

questions should be incorporated into a metrics program. By tracking and implementing specific improvements following an incident, an automotive company can build a body of knowledge to help it deal with future attacks.

4. *Follow cybersecurity core team best practices.* A best practice is to form a working group with permanent representatives from three critical groups—information or cybersecurity, legal, and corporate communications—that are responsible for dealing with incidents. Within this group, there should be a single leader who serves as response coordinator and is recognized as such by the entire group so there is no confusion, delay, or disconnected communications among team members.

   This core group should simulate its response to cyber incidents by walking through plans and procedures. These exercises can serve as part of a broader strategy for how to move swiftly and effectively in response to an attack. A typical simulation includes working through the severity matrix (from major to minor incidents) and relevant actions; collecting forensic data to help determine the nature of the attack; coordinating communications internally and externally; and discussing backup plans.

5. *Address supply chain risks.* Automotive companies need to monitor their partners' operations for potential security breaches and manage the access of users to different systems. Smaller vendors present special risks, since they tend to have less stringent security protocols, so contracts should include audit clauses and mandated testing procedures.

6. *Invest in advanced tools and technology.* State-of-the-art technology is needed to fight back against increasingly sophisticated threat actors and vectors as well as to mitigate the risk of valuable corporate data dispersion throughout organizations and supply chains. One way to stay current is to leverage the capabilities and infrastructure of subscription-based services that use the cloud. These services provide real-time updates that aggregate information and keep defenses fresh and dynamic. But it is equally important to deploy and configure tools that meet each organization's specific operating circumstances.

"By tracking and implementing specific improvements following an incident... build a body of knowledge to help deal with future attacks"

The automotive industry is facing significant challenges as connected cars become the norm and fully autonomous vehicles enter the mainstream later in the decade. These technologies are expected not only to transform the industry, but also create greater cyber risks with the potential to damage a company's reputation and financial future. To mitigate these risks, a company will have to instill its organization and supply chain with a cybersecurity culture that recognizes threats and adheres to processes for combating those threats. Companies can use cloud-based services to provide real-time updates that aggregate information to help keep track of the continuously changing threat actors and vectors. But they will also need to invest in the latest tools and technologies that can limit the damage of intrusion.

Fighting for cybersecurity won't be easy or cheap. But it will enable the industry and its customers to stay safely on the road.

Contacts

To have a deeper conversation about the subjects discussed in this article, please contact the following:

PwC - US Automotive Practice

Ray Telang
Partner, US Automotive Leader
Tel: +1 (313) 394 6738
ramesh.d.telang@pwc.com

Mike Lambert
Principal, Automotive Technology
Tel: +1 (248) 613 5601
mike.lambert@pwc.com

PwC - US Cybersecurity Practice

Rik Boren
Partner, Cybersecurity & Privacy,
Industrial Products Leader
Tel: +1 (314) 206 8899
rik.boren@pwc.com

Rob Shein
Manager, US Advisory
Tel: +1 (202) 445 4447
robert.j.shein@pwc.com

Editorial Contributor

Gloria Gerstein
Tel: +1 (212) 787 4607
gloria.gerstein@pwc.com

General inquiries

Diana Garsia
Senior Manager, US Automotive
Tel: +1 (973) 236 7264
diana.t.garsia@pwc.com

www.pwc.com/automotive

www.pwc.com/mobility