Booz | Allen | Hamilton

Commercial Solutions

BORROWING FROM THE BANKS

WHAT THE FINANCIAL SECTOR CAN TEACH AUTOMAKERS ABOUT VEHICLE CYBER SECURITY

BORROWING FROM THE BANKS

WHAT THE FINANCIAL SECTOR CAN TEACH AUTOMAKERS ABOUT VEHICLE CYBER SECURITY

Vehicle cyber security is no longer an option: It is a business imperative.

Challenges and opportunities of the connected vehicle

With headline-grabbing claims and government attention, cyber security has arrived on the automotive agenda. The challenge can seem daunting, but there's good news: The automotive industry isn't the first to face the cyber challenge. Although some issues are unique to vehicles—especially safety considerations—challenges such as securing an ecosystem of connected products and services mirror what other industries have faced. We can accelerate vehicle cyber maturity by learning from the successes and failures of the commercial industry that first tackled cyber security on a large scale—financial services.

By examining lessons learned from financial institutions and applying them to the automotive industry, we have identified the key steps to develop an effective vehicle cyber security strategy and organization. This paper provides specific recommendations for how to: Identify and empower a vehicle cyber security leader, build a hybrid team, develop capabilities for managing risk across the ecosystem, and use cyber security to drive larger cultural change. When executed expertly, vehicle cyber security becomes a key business enabler of the connected future and a competitive differentiator for automakers.

Vehicle cyber security and the OEM

The features and services offered by the connected vehicle, while presenting exciting new revenue streams, are also expanding the cyber attack surface. The automotive industry may not have faced a real-world vehicle cyber incident yet, but it is clear that attackers—especially state actors—have the offensive capabilities[1]. Moreover, non-state, criminal organizations are increasingly incentivized to exploit vulnerabilities on the connected vehicle. Considering the multi-year timeline and complexity of building a vehicle, OEMs should move aggressively to build a holistic cyber security program. Vehicles being built now don't just need to protect against the risks we see today; they will face a rapidly increasing threat landscape throughout the next decade on the road.

The technical challenges associated with securing the vehicle, particularly as over-the-air communications increase, are significant. But this isn't just a technical challenge: It is just as important that organizations begin with a strategy and organizational construct to support and help maximize technical solutions.

Indeed, for OEMs, the challenge with vehicle cyber security is as much about culture as it is engineering. Vehicle cyber security refuses to fall neatly into typical organizational categories. Supply chain, privacy, product development, enterprise IT, services, payment processing, legal—the list of relevant parties inside OEMs is lengthy. Beyond it, the expanding connected vehicle ecosystem represents an even larger group of suppliers, competitors, regulators, and partners. The challenge is clear: OEMs must rally internal and external stakeholders around a common vehicle cyber security mission, breaking down barriers, and, ultimately, protecting the functions and services that will be critical to their businesses going forward.

1 Alexander, General Keith B., "Statement of General Keith B. Alexander, Commander, United States Cyber Command before the House Committee on Armed Services, Intelligence, Emerging Threats and Capabilities Subcommittee," United States House of Representatives, 13 March 2013, page 3.

Learning from financial services

The financial services industry was among the first to address cyber security as a fundamental business need. And it remains at the core of their business operations. They learned the initial hard lessons, and industries maturing in the cyber security space can learn from their experience—both their successes and their shortcomings.

Although automotive faces its own unique environment, there are some notable similarities with the financial services industry:

- **The cyber challenge rapidly emerged.** Both industries went through a rapid change from physical product to electronic service. This shift created a large-scale introduction of cyber as a new business need.
- **Many started ahead of the problem.** Neither industry jumped to action after an unexpected, wide-scale attack. Academic papers cited vulnerabilities that adversaries could exploit, the government expressed its concerns, and the media popularized these views[2]. Both industries started to secure their businesses in reponse to early indicators that a lack of security could be devastating.
- **Cyber became a competitive advantage.** The emergence of the cyber challenge was accompanied by a shift in thinking: Cyber is the foundation for providing new, better, more convenient and more valuable products and services to customers. Security is a necessity to stay ahead of the competition and help companies thrive.
- **Hackers went big.** Both OEMs and financial services are an attractive target for threat actors. These companies have deep pockets, and they have broad reach. The potential scale and scope of an attack makes it a potentially profitable endeavor. The complexity of their connected systems also creates a huge attack surface. And all it takes is one vulnerability to get inside.

Although, financial services has had time-in learning, automotive is new to cyber. OEMs have an opportunity to take and reuse what's worked and to rework what hasn't.

Booz Allen has done work with most top US financial institutions to assess the maturity and performance of their cyber security organizations.

The Big Lessons

Financial services isn't perfect in their approach to cyber security. Attacks still disrupt operations. But, as one of the biggest targets of attacks, they have sharpened their approaches significantly throughout the years and are able to effectively minimize the effects of many attack vectors. During the last decade, banks have experienced numerous successes and shortcomings. And a clear set of select lessons has emerged for all industries facing the cyber challenge.

01 *Financial Services Cyber Security Snapshot*

Successes	Challenges
✔ Single accountable leader	✘ Cyber investments are often on a backburner until there is a breach
✔ Embedded security liaisons across partner/ related units	✘ Looking backward at historical incident analysis rather that predictive intelligence
✔ Dedicated team, with predefined surge support in case of an incident	✘ Inconsistent vendor management
✔ Cross-industry collaboration (FS-ISAC)	✘ Limited availability of cyber expertise and a competitve market for talent
✔ Extensive data collection and treat monitoring	

- **Deciding where cyber security fits is a first step.** There is no one-size-fits-all model. Cyber usually falls within a corporate core or operations team. Many leading companies place cyber organizations within their operations units; however, some that do not are still successful. Wherever the program resides, there is one critical element to make sure it is successful: There must be close coordination between the cyber security team, corporate core, and operations [3].

- **You're not just engineering a solution; you're fighting an enemy.** This is a fight against an adaptive and, at times, advanced adversary [4]. That's a different mindset for organizations that have traditionally been more accustomed to worrying about the competition. You need to defend your product with the right set of capabilities. This includes: Predictive intelligence; perimeter monitoring, wargames, exercises, and advanced security operation centers with access to multiple data sources and advanced analytical methods.

- **Technology alone won't solve the cyber security challenge.** Vehicle cyber security is too important to treat it exclusively as a technical problem. Only an integrative approach that balances technical solutions with business acumen can help realize the full potential of technical solutions—to reduce vulnerabilities and to best prosecute threats. A comprehensive risk management program, talent strategy, incident response protocol, and other organizational processes are key to success.

- **You don't need to go it alone.** An attack on one company affects an entire sector—and an attack at one institution is rarely an isolated event [5]. With all companies facing a similar threat landscape, there is value in pooling resources to monitor intelligence, analyze attackers, and share actionable information. The financial services sector learned this early on and stood up an Information Sharing and Analysis Center to enable mutually beneficial threat monitoring and intelligence sharing between participating companies [6]. It also facilitates knowledge transfer during and after incidents to help reduce associated consequences and improve security going forward.

---

3 New York State Department of Financial Services, Report on Cyber Security in the Banking Sector, May 2014, pages 6-7.
4 Snow, Gordon M., "Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit," Federal Bureau of Investigation, 14 September, 2011.
5 Crimmins, Danielle, Falk, Courtney, Fowler, Susan, et al., "U.S. Bank of Cyber: An analysis of Cyber Attacks on the U.S. Financial System," Purdue University Cyberforensics Laboratory, Spring 2014, pages 19-24.
6 Booz Allen Hamilton, "Information Sharing and Analysis Center: A Blueprint for Success," July 2014.

Every leader needs a team, and vehicle cyber security requires one of the best.

Translating to the auto industry

The experience of the financial services industry provides guidance for developing a strategy to take on vehicle cyber security. But the automotive industry also has distinct challenges. Foremost among them is the paramount importance of safety, which creates a lower acceptable level of vulnerability. For critical safety systems, there can be no tolerance for even minor cyber intrusion. And while bankers can focus on protecting server farms in their headquarters, limiting physical access, and identifying issues within their closely monitored and controlled network, automakers must protect vehicles that are sold and released "into the wild." Moreover, the complexity of the vehicle network architecture, the inability to rely on backup systems, the increasing interdependence with communication networks and consumer electronics, and the increased need for communication with infrastructure and other vehicles present a difficult set of variables to manage[7].

By working directly with OEMs as they confront vehicle cyber security, we know that supposed solutions that disrupt the business, assume vehicle cyber security can trump other organizational needs, or try to solve the problem by plugging in a few extra widgets will ultimately fail. What works is an overarching organizational strategy that empowers the right business leader to develop an approach for integrating cyber security across the vehicle lifecycle.

Borrowing from the financial services sector, but tailoring it to the needs of automotive industry, we recommend the following three-pronged approach: (1) Bring together the right team, (2) manage risk across the ecosystem, and (3) make it part of a bigger cultural change.

7 Staff of Senator Edward J. Markey, "Tracking and Hacking: Security and Privacy Gaps Put American Drivers at Risk," February 2015, page 3.

Bring together the right team

Identify and empower a vehicle cyber security leader

Someone needs to own this. Automakers need a single product cyber security leader, access to executive leadership, authority within the design and build process, and dedicated resources to protect vehicles. The vehicle cyber leader breaks down organizational barriers and takes accountability. This leader—the face of vehicle cyber security—champions cyber security from the boardroom to the factory floor to the showroom to the road.

Draft the right team

Every leader needs a team, and vehicle cyber security requires one of the best. The team's job is to build cyber security into the product ecosystem and the business. The team needs a product-centered approach that sits at the intersection of information technology and engineering. Look from within, as there is not yet a subset of vehicle cyber security experts readily hirable. Also engage externally, finding the security experts who may not have automotive industry experience but want to take on a new challenge—and do so with an understanding that their approach may challenge your culture. This is an evolving risk, so new thinking should be welcomed to challenge the status quo. The team should build a network across the OEM, interfacing with teams that deal with safety, reliability, privacy, supply chain, and customer service, among others.

02 *Designing a Vehicle Cyber Team*

	Leadership	Organization
Initial Action	Introduce a **vehicle cyber security leader**—a senior individual responsible for directing a dedicated vehicle cyber security organization and interfacing with the most senior managers of the business.	Establish a **dedicated vehicle cyber security organization**—complete with personnel, budget, defined functions, etc.—that drives enterprise-wide vehicle cyber security efforts through direct implementation and coordination across the company.
Responsibilities	• **Drive strategy**—development and execution • **Be the integrator**—unite vehicle-related security functions and embed them across product lifecycle • **Serve as the vehicle cyber "voice"**—at highest orders of the business (and externally) • **Lead incident response**—for vehicle-related cyber incidents	• **Manage cyber risk to the vehicle ecosystem**—maintain situational awareness of risks, implement security controls, and respond to incidents • **Establish/mature company-wide vehicle cyber functions**—operate core functions and align/integrate other functions (e.g. IT, supply chain) • **Communicate and engage**—with internal external stakeholders
Key Attributes	• **Executive presence** • **Business savvy** • **Large-scale transformation expertise** • **Balanced perspective of security and products**	• **Balance of expertise**—the team should include IT staff, product developers, engineers, software designers, security, and privacy experts • **Dedicated staff**—embedded or matrixed, with reach across business units

Manage risk across the ecosystem

Map the ecosystem

There are no cyber security solutions that work in isolation. Automakers must map the complete connected vehicle ecosystem to understand everything that "touches" the connected vehicle. This helps visualize the full attack surface—the technical, process, and human vulnerabilities that can be exploited to access the connected vehicle. With a complete picture of the ecosystem, organizations can map out where their risks lie as well as the security controls in place to reduce those risks[8].

When mapping the ecosystem, OEMs should consider the following areas:

- **Connected vehicle components**—the on-vehicle electrical components and features that control safety-critical systems, provide "comfort" experiences, and connect with external technologies and services
- **Vehicle lifecycle**—the end-to-end activities required to design, source, manufacture, sell, operate, and service a vehicle fleet
- **Enabling infrastructure**—the back-end and roadside information and communication technologies and services that capture and send data to and from the vehicles, allow for vehicle fleet monitoring, and provide on-the-road services
- **External influencers**—the array of individuals and organizations—including consumers, government entities, direct and indirect competitors, industry forums, the media, and threat actors—that can shift the connected vehicle business model and operations

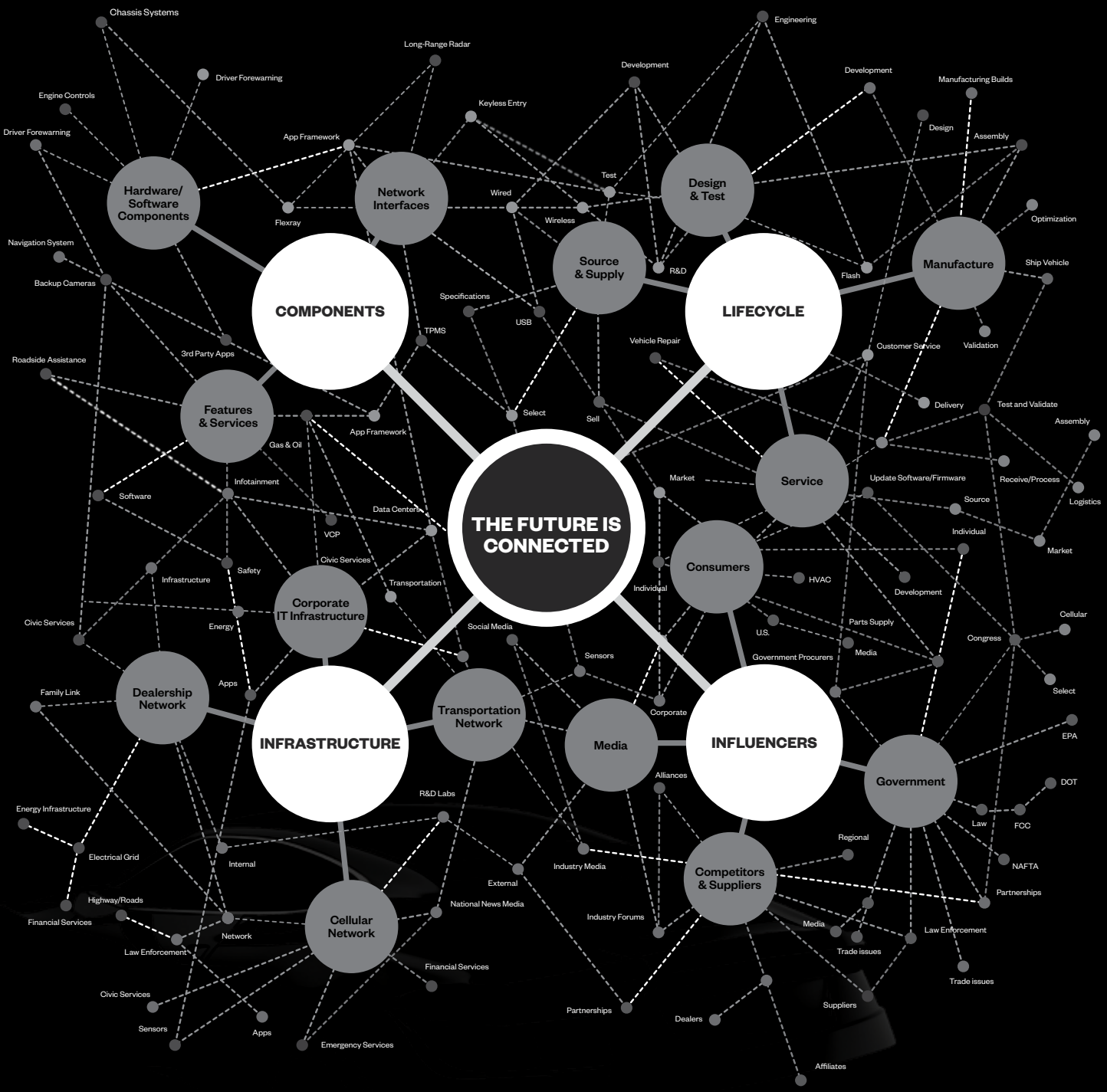
Understand the scope

OEMs have built in numerous technical solutions—encrypting communications and segregating connected components—to minimize vulnerabilities that adversaries could exploit. But the automotive business model is shifting. It's not just about building and selling a secure product: It's also about maintaining a relationship with the customer throughout the full vehicle lifecycle. Automakers are beginning to address this evolution, taking ownership of security services after vehicles leave the lot. For example, a growing number of OEMs are developing on-vehicle continuous monitoring and detection capabilities and frequently resolve newly identified issues with software patches[9]. This combination of security technologies and services is important for protecting the vehicle and reducing vulnerabilities.

8 Booz Allen Hamilton, The Connected Vehicle Movement, 2014.

9 Lucas Mearian, "Over-the-air software coming soon to your next car," ComputerWorld, 05 February 2015.

03 *The Connected Vehicle Ecosystem*



Build a network of sensors across the connected vehicle ecosystem to capture early indicators of vulnerabilities, attack methods, and malicious actors.

Identify threat actors

After an initial inward-looking analysis, organizations must look outward to understand the threat landscape. We recommend building a network of sensors across the connected vehicle ecosystem to capture early indicators of vulnerabilities, attack methods, and malicious actors. Look across industries to identify the methods, resources, and intentions of various threat actors. One of the best ways to learn more is to go where they are: Deep Web collection can identify potential adversaries in underground forums and illicit networks that are not indexed or accessible through typical Internet search engines.

Manage risk with analytics

With an understanding of the ecosystem and the actors within it, cyber security experts can more readily identify threats and vulnerabilities. Effective vehicle cyber security programs require advanced analytics to monitor threats, identify incidents early, and mitigate risk. Work with IT enterprise security to build a continuously updated library of algorithms that detect patterns of anomalous behavior and alert key cyber staff to evidence of a threat actor's presence within your network, supply chain, or vehicles. Build an analytics platform that provides the speed necessary to keep pace with threats as they evolve. In the murky world of cyber security, data analysis helps to answer the skeptics' questions of "so what" and "why should we care" with accurate impact assessments and actionable intelligence.

Make it part of a bigger cultural change

Even with the smartest team and advanced capabilities, vehicle cyber programs will fail without full support. In part, full support means a dedicated budget and decision authority. But it is also about organization-wide awareness and commitment to vehicle cyber security. This entails a supportive culture that understands the intrinsic relationship between cyber security, the future of the product, and the business. Managing change—the new organization, the new way of looking at the vehicle, and the introduction of new capabilities—is critical.

The most effective way to manage this change is by talking about vehicle cyber security as an enabler. After all, these efforts are not just about compliance or securing parts. This is about transforming your business—enabling connected products and services, making processes more efficient, building industry-leading analytical capabilities, and committing to protecting your customers while providing them with new value.

There are three key enablers to help frame this argument.

Insights to improve the customer experience. In a world of distractions and competing screens, you have the coveted "captive consumer." Firms pay billions to buy makers of products that provide access to user preferences and data. By providing a product to users, automakers automatically have that access at no cost. Leveraging Big Data analytics, OEMs have the chance to gain real insights into how consumers use their vehicles and services, which can help prioritize R&D efforts that improve the customer experience.

Ability to increase revenue through on-vehicle services. Cyber security positions automakers to take advantage of the growing demand for connectivity and to integrate with the Internet of Things to create entirely new services.

A new way to talk about quality. Consumers consider a range of factors when purchasing a vehicle, including safety ratings, reliability, comfort, design, and services. Automakers have the opportunity to add cyber quality to this list. Cyber security is critical to ensuring vehicle safety and builds trust around using new vehicle services by protecting personally identifiable information (PII) and credit card information. Making cyber security part of the brand gives consumers confidence in their purchase.

Organizations that clearly talk about the positive business values of cyber security are better able to shift the culture toward supporting the initiative, rather than just seeing it as another disruptor or an add-on responsibility of team members' jobs. After tailoring these messages to your business, it's important to share them through multiple channels—through new required cyber awareness courses and annual refreshers, team meetings, internal and external marketing campaigns, and other internal communication mechanisms.

Why now?

Building the right approach for vehicle cyber security is important for the future of automotive. It's a business enabler. When done well, a vehicle cyber security program will be part of a larger business transformation—enabling the connected services and increased automation that underpin the evolving relationship with customers.

Organizations that find the creativity and flexibility to tackle vehicle cyber security will be best positioned to keep pace with the speed of innovation, competitive pressures, and game-changing revenue opportunities in the connected era. Whichever OEM finds the most value from data—for their customers and their businesses—will find a significant competitive advantage. The vehicles that make the most of connectivity—with increased automation and new services—will see an increase in sales, especially on higher-end platforms. A vehicle cyber security program that maintains trust with drivers and reinforces brand quality makes sure these opportunities are realized.

With the right leadership and an integrated approach, OEMs will find that this opportunity outweighs the risks. And now is the time to act.

To learn how Booz Allen Hamilton can help your business thrive, contact:

Sedar M.T. LaBarre
Vice President
labarre_sedar@bah.com
Tel +301-452-4996

Jon Allen
Principal
allen_jonathan@bah.com
Tel +703-377-7194

Denis Cosgrove
Senior Associate
cosgrove_denis@bah.com
Tel +202-346-9296

Alexandra Landegger
Associate
landegger_alexandra@bah.com
Tel +202-340-8308

www.boozallen.com/commercial

Booz | Allen | Hamilton

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. The firm provides business and technology solutions to major corporations in the financial services, health, and energy markets, leveraging capabilities and expertise developed over decades of helping US government clients in the defense, intelligence, and civil markets solve their toughest problems. Booz Allen is headquartered in McLean, Virginia, employs more than 22,000 people, and had revenue of $5.48 billion for the 12 months ended March 31, 2014. In 2014, Booz Allen celebrated its 100th anniversary year. To learn more, visit www.boozallen.com. (NYSE: BAH)