Information Technology in the Automotive Aftermarket

AASA Special Report

AASA Thought Leadership:

Information Technology in the Automotive Aftermarket

The following white paper consists of key takeaways from three AASA surveys conducted in 2014, which focused on information technology in the automotive aftermarket. In addition, similar research from PwC was also included.

The key reports include the AASA Technology Council Cyber Security Report, PwC's Managing Cyber Risks in an Interconnected World, the AASA Technology Council IT Benchmarking Survey and the 2014 Q3 Quarterly Barometer with special questions focused on "cataloging in the aftermarket."

Produced and edited by:

- *Chris Gardner, AASA Vice President*
- *Bailey Overman, AASA Senior Analyst of Industry Analysis*
- *Krysta Messier, AASA Junior Analyst of Industry Analysis*

If you are interested in receiving more information on any of the abovementioned reports, please contact Curtis Draper at cdraper@aasa.mema.org or Bailey Overman at boverman@aasa.mema.org or Krysta Messier at kmessier@aasa.mema.org.

The following report contains key high level takeaways from the full survey.

AASA Technology Council Cyber Security Report

Is your company well defended against cyber-attacks? If your answer is yes, you are rare among your aftermarket supplier peers. Only one of five participants in the AASA Technology Council (ATC) cyber protection survey believes their intrusion detection system is effective for their company.

ATC initiated this survey in June 2014 to identify key issues and “pain points” on cyber protection and compliance for aftermarket suppliers. Survey participants can use the full survey report to benchmark their company’s state of cyber security against other suppliers.

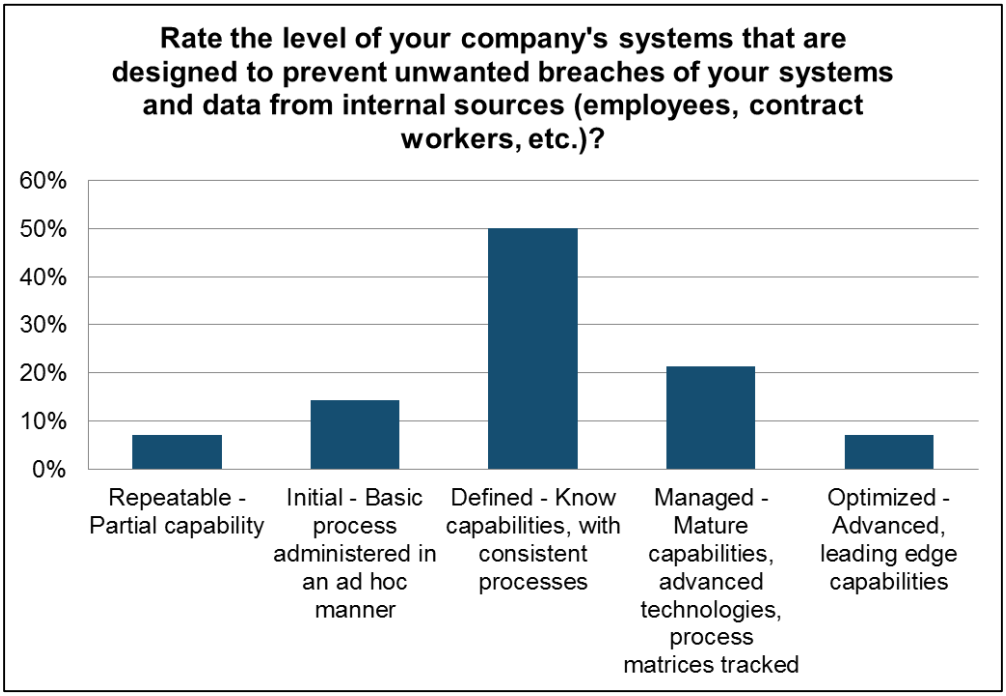
The full report is only available for participating companies, but results were discussed at the 2014 AASA Technology Conference, October 5-7, in Marco Island, FL.

The 2014 conference highlighted how current and emerging technologies will drive efficiencies, reduce costs, identify customer trends and forecast future needs.

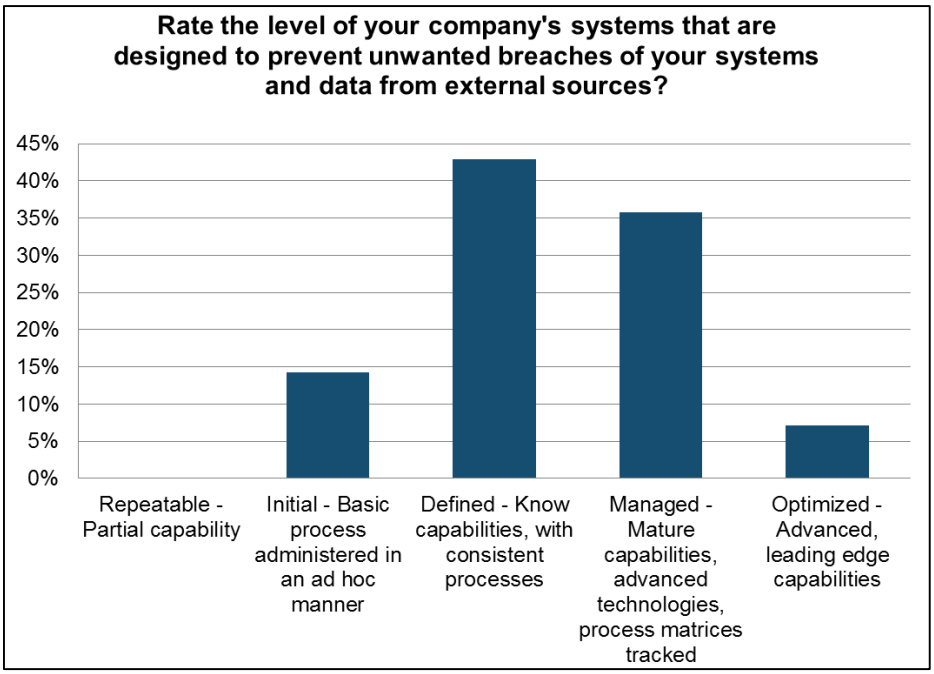
Contact Chris Gardner at cgardner@aasa.mema.org or 919-406-8830 with any comments on or questions about the survey, the Technology Conference or about the AASA Technology Council.

Capability of Security for Unwanted Breaches by Internal and External Sources

When asked about their company's security systems that were designed to prevent unwanted breaches from internal sources, only 28% of respondents have a high level of capability in their current system, meaning the majority do not have either a managed or optimized security system, leaving opportunities for aftermarket suppliers to upgrade their systems to achieve a higher capability of security.

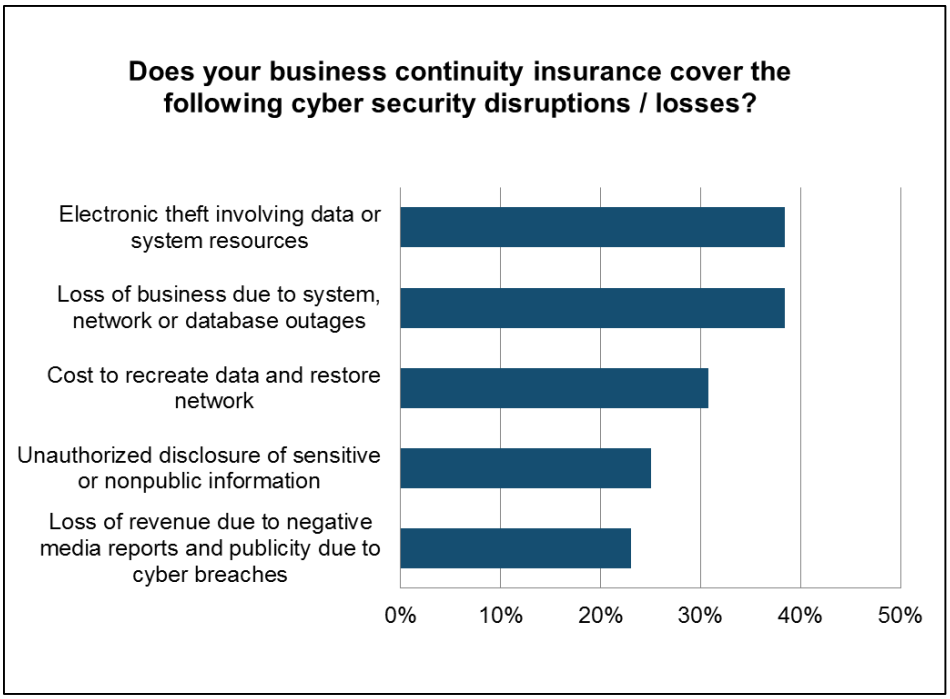


When asked about breaches from external sources, 43% of respondents indicated they had a “Managed” or “Optimized” system to prevent breaches from external sources. This shows that aftermarket companies focus more on threats from external sources than internal ones. Many industries also focus more heavily on external breaches but with recent and heavily publicized breaches of internal information as seen in the Pvt. Manning and Richard Snowden cases, changes could be seen in the future in terms of information security.



Disruptions and Insurance Coverages in a Cyber-Attack

When a breach or cyber-attack did occur, “product and application data” was found to be the most at risk, followed by lost productivity and loss of revenue. For those who have business continuity insurance, “electronic theft” and “loss of business due to outages” were the top issues covered. Surprisingly, none of the options were covered for a majority of respondents.



Managing Cyber Risks in an Interconnected World

Cybersecurity is now a persistent business risk as seen in Pricewaterhouse Coopers' (PwC) release titled Managing Cyber Risks in an Interconnected World, key findings from The Global State of Information Security® Survey (GSISS) 2015.

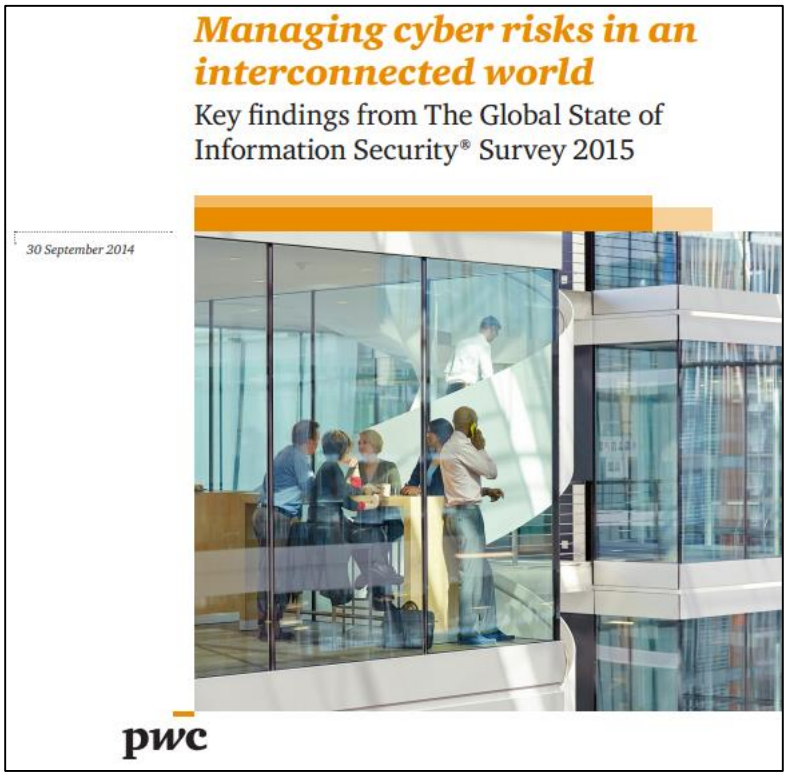
A report issued by US Sen. Edward J. Markey last week [Feb. 9] calls for automakers to establish security standards to address the possibilities of attacks on Internet-connected vehicles. The gist of the report, which is based on responses from 16 global auto manufacturers, is that carmakers haven't implemented safeguards to protect drivers from cyberattacks or invasions of privacy.

As the report pointed out, security experts have proved that hackers can remotely access the computer systems of connected automobiles and control vehicle components like the brakes, or steal private customer data collected by on-board computers. As a topic, attacks on connected vehicles can produce sensational headlines, however, no car has been commandeered by hackers.

Of more immediate concern to automakers is the broadening array of adversaries that are accelerating attacks on their sensitive data, networks, and trade secrets. In fact, GSISS 2015 found that automotive companies reported a 32% increase in detected security incidents in 2014.

Contact Chris Gardner at cgardner@aasa.mema.org or 919-406-8830 if you would like to receive a copy of PwC's key findings on specifically the automotive industry from GSISS 2015.

Contact Dennis Wojdyla at dennis.wojdyla@us.pwc.com with any comments on or questions about the survey or how to obtain a full copy.



As incidents rise, automakers have more to worry about than car hacking

A report issued by US Sen. Edward J. Markey last week [Feb. 9] calls for automakers to establish security standards to address the possibilities of attacks on Internet-connected vehicles. The gist of the report, which is based on responses from 16 global auto manufacturers, is that carmakers haven't implemented safeguards to protect drivers from cyberattacks or invasions of privacy.

As the report pointed out, security experts have proved that hackers can remotely access the computer systems of connected automobiles and control vehicle components like the brakes and steering, or steal private customer data collected by on-board computers. Articles and news segments on the Markey report stress that risks will increase as more in-vehicle devices are connected to the nascent Internet of Things.

As a topic, attacks on connected vehicles can produce sensational headlines. To date, however, no car has been commandeered by hackers, nor are there incentives or a business model to do so.

Of more immediate concern to automakers is the broadening array of adversaries that are accelerating attacks on their sensitive data, networks, and trade secrets. In fact, The Global State of Information Security® Survey found that automotive companies reported a 32% increase in detected security incidents in 2014.

And while compromises attributed to hackers inched up, insiders like current and former employees remain the most frequently cited culprits. Not all insiders are employees, however. Automotive executives are increasingly worried about threats that can arise from sharing networks and data with third-party business partners. They know that these partners—supply chains, in particular—can be a weak link through which adversaries gain a foothold on the organization's ecosystem for long-term exfiltration of important business data.

In 2014, more than half (57%) of automotive respondents attributed security incidents to these outside insiders. Yet we found a pattern of inattention: Consider that only 52% of respondents say they perform risk assessments on third-party vendors and just 57% have established security baselines and standards for third parties.

We also noted a spike in compromises attributed to competitors. Increasingly, automotive executives worry that rivals—including those backed by nation-states—are infiltrating their networks to pilfer trade secrets, product designs, and sensitive communications. Another concern is that these threat actors may convince financially motivated employees to leak valuable business information

Given the increase in detected incidents and the frenzy of media reports on car hacking, we were surprised to learn that many automobile companies have trimmed their information security budgets. In fact, security spending declined 16% in 2014. That may not augur well for automotive security efforts in the coming year.

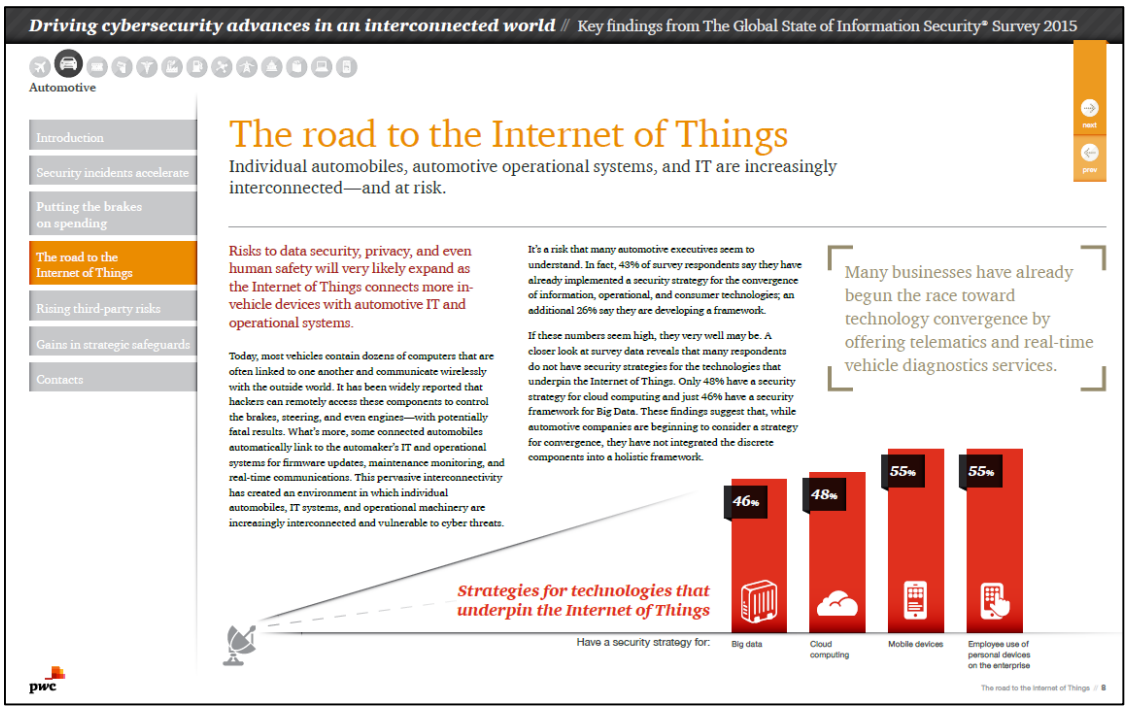
On the road to the Internet of Things

By now, it is accepted that risks to data security, privacy, and even human safety will expand as the Internet of Things connects more in-vehicle devices with automotive IT and operational systems. These threats will no doubt move from concept to reality as automotive companies race toward the Internet of Things without a firm security strategy in place.

Already, almost half (45%) of respondents say they produce or sell in-vehicle products or services that enable telematics, and 61% report they are involved in interactive, real-time vehicle-system diagnostics services. Not all have worked out the security and privacy details, however. When asked if they are positioned to securely provide the services they already offer, 31% of respondents say they were not or did not know.

If media coverage of car hacking and the Internet of Things has an upside, it's that headlines have helped jumpstart formation of the Auto ISAC (Information Sharing and Analysis Center). The ISAC should encourage more automotive companies to share security information and gain actionable intelligence on threats and response tactics. It's an approach that automotive companies are already embracing. Among survey respondents, 58% said they collaborate with others to improve security intelligence and tactics. That's an advance over last year, and the commitment to collaboration will likely continue to grow as awareness of risks continue to make news.

The fact is, cybersecurity will become increasingly challenging as more electronic data is shared among a widening ecosystem of partners and original equipment manufacturers (OEMs). Consumer demand, too, will drive implementation of new in-vehicle technologies and services. Automotive companies will need to develop an integrated security strategy that balances threats with protracted component testing timelines and product lifecycles. In addition to advanced technologies, strong, proactive processes will be essential.



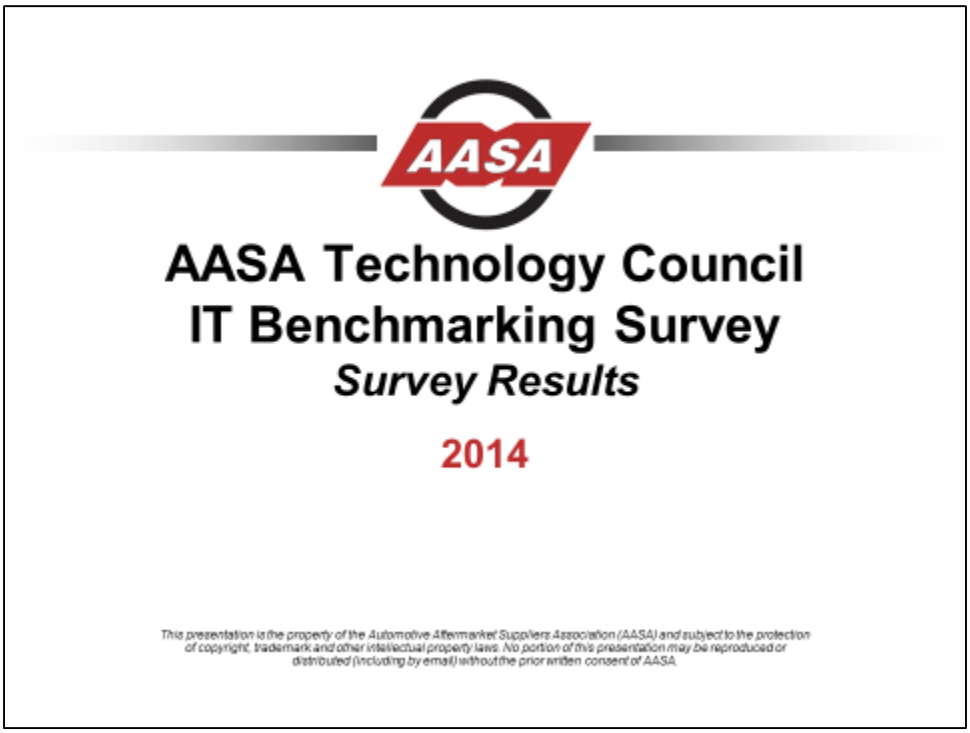
AASA Technology IT Supplier Benchmarking Survey

The ATC conducted its third annual IT Supplier Benchmarking Survey in 2014 and compiled an information and insight heavy report. The survey addresses critical information areas that impact suppliers' planning, ability to deliver efficient processes and ability to meet customer needs.

AASA members are able to benchmark their information environment and priorities against the aftermarket supplier industry and other industries.

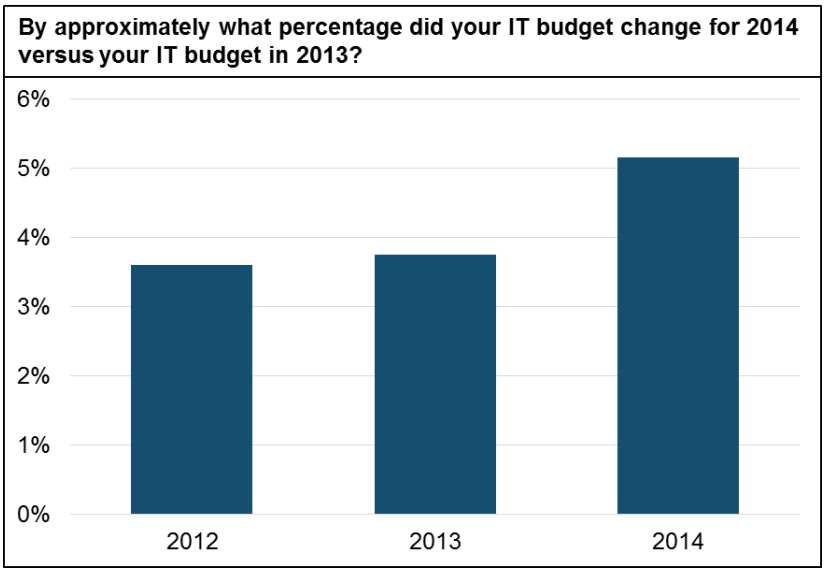
Results can provide valuable information for planning, budgeting and development of the future direction of technology for manufacturers.

Contact Chris Gardner at cgardner@aasa.mema.org or 919-406-8830 with any comments on or questions about the survey or about the AASA Technology Council.



IT Spend and Forecast

Despite IT budgets remaining steady from 2013, the majority of aftermarket IT executives indicated an increase in their budgets from the previous year, the highest average growth rate since 2012, stressing the growing importance of IT in the aftermarket industry. The majority of respondents also indicated that demand for aftermarket IT at their companies was rising.



IT Performance

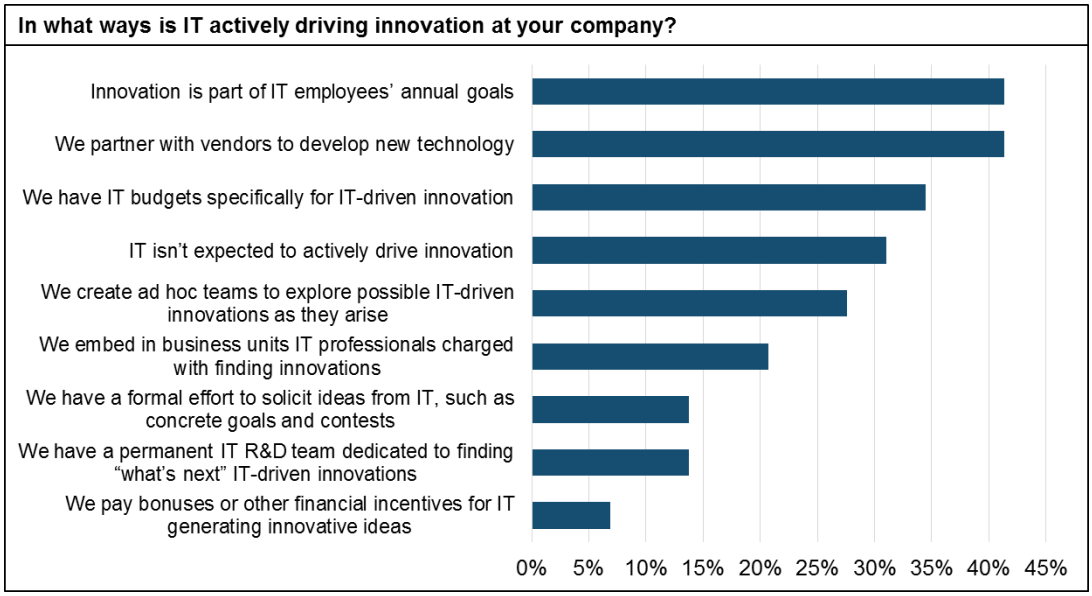
The majority of respondents indicated that their aftermarket IT team interacts most with customers when shaping mobile strategy which reiterates the importance of mobile strategy for the automotive aftermarket going forward. “IT leaders are on the team shaping mobile strategy” ranked higher for aftermarket IT than for other industries although data analytics were also important for both aftermarket IT and other industries.

Which of the following apply to your IT team’s interaction with the company’s customers?

Aftermarket IT	Other Industries
1. **IT leaders are on the team shaping mobile strategy**	1. **IT partners with marketing and other departments on analytics initiatives**
2. **IT partners with marketing and other departments on analytics initiatives**	2. CIO regularly visits customers
3. IT leaders are on the team shaping social media strategy	3. **IT leaders are on the team shaping mobile strategy**

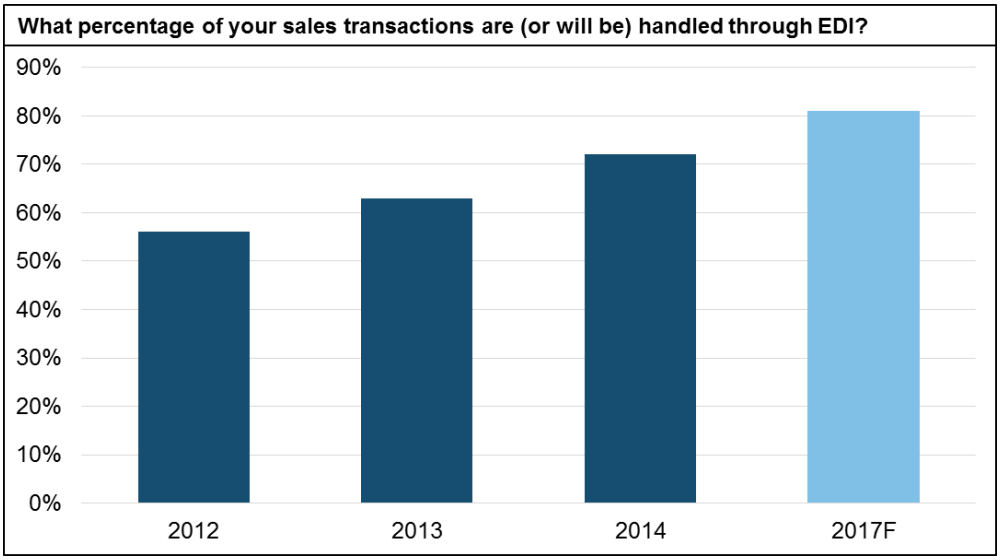
IT Innovation

Aftermarket IT actively drives innovation by incorporating it into annual goals and partnering with vendors to develop new technology. The majority of aftermarket IT respondents are planning to innovate this year by making business processes more efficient. “Deploying tablet computers or mobile devices” and “Expanding analytics & business intelligence” were the top initiatives being implemented by aftermarket IT.



Aftermarket-Specific Technologies/Standards

Average percentage of sales handled by EDI are projected to increase from 2014 to 2017. EDI for aftermarket IT has seen steady growth over the last 3 years. Average percentage of sales handled by IPO projected to increase as well from 2014 to 2017.



AASA 2014 Q3 Quarterly Barometer Special Questions

Every quarter the AASA Industry Analysis team conducts a barometer to gain market insights on suppliers' outlook, sales trends, pricing and margin changes, hiring trends, sales inventory levels and how your company's performance compares to the market and peers.

The special questions for 2014 Q3 focused on cataloging in the automotive aftermarket. Questions regarding ACES, PIES and other formats were asked to determine what suppliers use as their standard.

Participation in the AASA Quarterly Barometer is the only way to receive a copy of the quarterly report and aggregated results in addition, to a PowerPoint with easy to grab slides for management presentations. Please note that all responses are confidential.

Contact Bailey Overman at boverman@aasa.mema.org with any comments on or questions about the survey or how to sign up to be involved in next quarter's barometer.

Cataloging in the Automotive Aftermarket

When surveyed, an average of 72% of respondents' customers requested product data in the ACES format. However, a majority of the respondents, 58%, also indicated that they prepare and deliver customer data in formats other than ACES such as PIES. The top reasons for not providing ACES to all customers was due to "discrepancies in the data" and "missing vehicles."

An average of 72% of respondents' customers request vehicle application data in ACES format, and 57% of their customers request product data in PIES format.

Aftermarket supplier respondents believe they do the best job providing data to "Retailers." e-Tailers ranked second. About a quarter of companies use third party companies to map their data to customer requirements for PIES and ACES.