
Purpose of ACRA: To have a more profitable and better managed collision repair business through education.



Arkansas Collision Repair Association

October 2010

SEPTEMBER EDUCATIONAL PROGRAM

The September Educational Program was presented by Mr. Dana Haswell of Aerotek, a General Motors contractor. Mr. Haswell is a Powertrain and Collision Specialist SCR. General Motors has a Conquest Parts Program and Bale Chevrolet of Little Rock is a participant in this program.

Have you ever been caught between wanting to use a GM OEM part and an insurance estimate that calls for an aftermarket part? This is usually because the aftermarket part is less expensive than the OEM part. Mr. Haswell said that under the GM Conquest Program GM Dealers have the ability to discount program parts up to 33% off Keystone's list price. Typically the most popular parts are copied by aftermarket manufacturers. The GM Conquest Program currently has over 3,500 parts that qualify and these include sheet metal, lighting, structural parts, and brackets.

First a body shop must have an estimate written by or on behalf of an insurance company that specifies NON OE parts: aftermarket, used, remanufactured, refurbished, Like Kind Quality. Next you fax the entire estimate to your GM dealer. The estimate needs to show the insurance company name or policy number. The GM dealer will "scrub" the entire estimate for eligible parts and send you a quote. You

can cross out any personal or private information on the quote.

Mr. Haswell gave this example:

GM part list price	\$268.35
Aftermarket list price	\$227.98
Less 33%	-\$75.23
YOUR COST FOR GM PART:	\$152.75

After you convert the aftermarket to OE parts you mail in supporting documents to marketing headquarters. About 8 weeks later you will receive by mail a Visa Gift Card. The claim form is simple to complete and takes very little time. Mr. Haswell can be contacted at 901-652-0295 and will be happy to help with questions and/or procedures.

Helpful GM Websites include:

GMRESTORATIONPARTS.COM

GOODWRENCH.COM

TECHINFOR.GMGGOODWRENCH.COM

ACDELCOTECHCONNECT.COM

Note: We have invited the Pulaski Technical College Collision Repair Department to attend the monthly ACRA meetings. In September we had 30 people in attendance and about half were new students.

OCTOBER AND NOVEMBER EDUCATIONAL PROGRAM

The October 12th Educational Program will address the 'Six-H Rule', which definitely affects Arkansas body shops, and will be presented by the Arkansas Department of Environmental Quality.

Mr. Doug Schlueter, I-CAR South Central Regional Manager, will present the November 9th Educational Program. As most of you are aware, I-CAR has recently changed part of their programs.

Mr. Schlueter will address certification issues. One of the benefits of membership in ARCA is that each year every ACRA member can send one person to an ACRA sponsored I-CAR class, usually held in June of each year.

SHOP OWNER SHARES HIS VIEW ON PARTS

Mr. Aaron Schulenburg of SCRS wanted to share with you a viewpoint from one of SCRS' members out of Iowa, that was published over the weekend in John Yoswick's CRASH network. Mr. Schulenburg spoke with Mr. John Arnold and he asked me to pass this along. The letter is as follows:

I have been reading with great frustration the recent news articles regarding non-OEM parts. There are opinions circling the globe, yet I don't feel one has expressed the opinion of the independent shop owner.

I have been involved in the collision repair industry for 40 years. I am old enough to remember the serious debates the industry faced as the first "re-chromed" bumpers appeared in the marketplace. The suppliers convinced the insurance industry that the "revitalized" product was an acceptable replacement bumper at a lesser cost. The body shops were convinced that the product was inferior and were able to prove on many occasions that the bumpers fit poorly. (At the time, I used to mark the rejected bumpers on the inside to see if they were sold to me again. Some were.) The chrome would peel on some of the product and I would have a warranty discussion with the supplier and sometimes the insurance carrier.

As time passed, the quality improved to the point where the re-chromed bumper was often a better product than the OEM. (My supplier would copper plate the core prior to the chroming process.) Eventually, I found myself telling the customer that "quality" was not necessarily synonymous only with OEM - and on many occasions, the alternative was a better product with a longer warranty.

As "rubber" bumper covers appeared, I went through the same agonizing process. However, the aftermarket covers never achieved the popularity that the "re-chromed" bumper did. (In fairness, I remember when an aftermarket cover on a specific brand fit better than the OEM cover did.) I found myself informing my customers that the quality of the parts was in many cases inferior to OEM.

My first experiences with non-OEM bolt-on sheet metal convinced me it did not meet my quality standard. The non-OEM suppliers made a decision that alienated them from any type of customer-service relationship with the body shop industry: They promised the insurance industry that the non-OEM part was of equal quality to the OEM version. I think the supplier forgot that the body shop was their customer.

A certification entity appeared to alleviate the quality concerns with non-OEM sheet metal. Some insurance companies would offer "lifetime warranties" on the bolt-on non-OEM sheet metal to the vehicle owner. But in my experience, non-OEM sheet metal parts destroy any chance of achieving a promised delivery date to a vehicle owner. Fit and finish of the non-OEM part has always been an issue. Some of the parts present liability concerns for the body shop and safety concerns for the vehicle owner.

In my own shop:

- I do install some non-OEM sheet metal on my customer's vehicles. The key is upfront disclosure and truthfully setting the customer's expectation prior to the beginning of the repair.

continued on page 3

- I hear my staff telling an insurance person that a part does not fit correctly and the end result will be a poor quality repair. I hear the insurance person tell that staff person he/she needs to discuss this with the supplier, who has told the insurance industry that their parts will fit.

- I returned one-third of the non-OEM body parts I purchased from my supplier in the first six months of 2010. The majority of those parts were returned because they were not acceptable due to a fit or finish issue.

- This means that 67 percent of the non-OEM exterior body parts we purchased were installed. In most cases, my technicians spent additional time to make these parts meet my quality standard. This is time that is not recoverable from an insurance carrier (but may be recoverable from my supplier).

- Over 10 years ago, I would back-charge my supplier for the additional labor involved in fitting a non-OEM exterior body part. Eventually, the supplier told me the part I was ordering was not available. I would tell the insurance company what the supplier said. The insurance company would call the supplier and be told the part was available. I had a choice to make: repair the vehicle with the non-OEM part, or another shop would repair the vehicle.

- It is my experience that “cycle time” suffers using non-OEM parts.

The controversy has grown as non-OEM structural body parts are now being offered. One example of this is a plastic radiator support being sold as the replacement for a magnesium support, as reported in the national trade press. There is a crystal clear safety issue with this plastic replacement part.

The number of customers to serve and vehicles to repair is decreasing each year. The insurance industry and the body shop industry are suffering financially because of forces beyond their control. The vehicle manufacturers are caught between CAFE standards and providing smaller, lighter-weight vehicles for an aging, overweight population demanding creature comforts. The salvage markets are driven by foreign investors and “under the radar” vehicle repairers.

To all these segments of the industry: Where does the madness end? As a group, we have all churned the repair of a vehicle into a legal and political nightmare. We have lost the focus we all need to reclaim: The key to the customer service we all strive to offer is upfront disclosure of the details of every transaction and truthfully setting the customer’s expectation based on facts prior to the beginning of the repair. If the customer does not agree with the end result of the repair process, they will respond accordingly.

John Arnold
Arnold’s Body Shop
Davenport, Iowa

PULASKI TECH RECEIVES \$200,000 TO ENDOW AUTO SCHOLARSHIP

Bumper to Bumper Auto Parts/Crow-Burlingame Company has committed to donate \$100,000 to endow the scholarship, and the college will receive another \$100,000 in matching funds through a U.S. Dept. of Education Title III grant, for a total of \$200,000. The gift was given in celebration of Crow-Burlingame’s 90th anniversary in the automotive parts industry. Other vendors contributed to Crow’s gift and include ACDelco, Moog Chassis Parts, Standard Ignition Parts, Quality Build Starters and Alternators, WIX Filter Co, Gates Rubber Co., Continental Batteries, Alliance Parts Warehouse, NGK Spark Plugs, DuPont Paint, PPG Paint, and Castrol Oil Co.

The scholarships will be awarded to a second-year student who shows commitment to completing certification in a transportation technology-related program and a desire to have a career in the automotive repair profession. The first scholarships will be awarded as early as the fall 2012 semester. The federal matching funds will be invested and allowed to grow for 20 years before scholarships are awarded from the income earned. More than 200 students are currently enrolled in transportation technology-related programs, including 106 students in automotive technology, 45 in collision repair technology, 46 in diesel technology and 21 in motorcycle/ATV repair technology.

CATCHING THE CLOUD: MANAGING RISK WHEN UTILIZING CLOUD COMPUTING

By ERICH BUBLITZ

Cloud computing has become a vitally important part of the information technology landscape.

A recent survey by London-based independent research firm Loudhouse found that approximately 51 percent of organizations are now utilizing cloud services as part of their IT infrastructure. There is growing concern, however, that cloud computing poses a security risk, and that risk is being debated throughout the technology community. (Results of the June 2010 Loudhouse survey are available at <http://www.mimecast.com/barometerresearch2010>.)

WHAT IS IT?

The term “cloud computing” refers to the practice of “outsourcing” a portion of a company’s technology environment to a shared third-party environment. Although the terminology is relatively new, cloud computing is not an entirely new concept. In the past, similar offerings were known as “application service providers.”

Some common examples of cloud computing include Salesforce.com, a company that can fully host its clients’ customer relationship management (CRM) needs, or Google’s Gmail platform for businesses, in which the client’s e-mail environment exists almost entirely within Google’s systems rather than onsite at the business.

UNDERSTANDING THE RISKS

One of the most common questions related to cloud computing is: In what ways does reliance on cloud computing expose a company to additional risk? The simple answer is that there is no simple answer.

While there are valid concerns, this may not be the appropriate question for many organizations. The issue is a moot point for many companies as the services they can obtain through a cloud environment simply are not obtainable otherwise, as a result of the cost and complexity of replicating those services internally. Indeed, the use of cloud computing has

become so pervasive that the Obama administration has launched a Federal Cloud Computing Initiative to identify possible cloud computing applications across the federal government.

That means that most companies need to focus their energy not on debating whether to embrace the cloud model but rather on managing cloud computing appropriately so that the risks are mitigated.

In order to appropriately manage the security risks of cloud computing, an organization must come to the realization that outsourcing functions to a third party is not the same as outsourcing the risk.

Cloud-based services too often are perceived as an opportunity to buy service that doesn’t have to be managed. But this fallacy is the greatest risk to any company that is utilizing services within the cloud. While the data may be residing on another company’s systems, the responsibility for that data has not fully transferred to the cloud service.

If a company that sells widgets online is using a hosting company like Rackspace Hosting to host in the cloud, that fact is likely to be invisible to the customers. They are entrusting, and holding accountable, the widget retailer, not Rackspace.

In March 2009, Google experienced a security flaw with their Google Docs service, an online service that allows creating and saving documents over the web. Documents that were set not to be shared were being shared due to a coding error by Google.

While Google estimates that only .05 percent of documents were affected, the number of documents stored on Google’s service is massive. Though no one is sure of the impact, even one document leaking from this error containing a customer list, Social Security numbers, or other sensitive information could cause the user thousands if not millions of dollars in first- and third-party expenses.

continued on page 5

Any company that chooses to use cloud computing should treat the cloud provider just as they would any other independent contractor or vendor it hires. This means:

- Actively managing the provider
- Reviewing contracts
- Securing indemnity
- Understanding the vendor's security practices
- Thinking through the insurance implications

SECURITY PRINCIPLES

The first principle to effective cloud security is to remember who has responsibility to the customer. Companies are responsible to their users regardless of whether or not they are utilizing a cloud provider or any other independent contractor. It is their names that will be published, their offices that receive calls from unhappy customers, and their cost (at least initially) to remediate the issue.

All decisions should be made with the thought that they are still responsible even when the data lives in the cloud. It is important to realize that things can go wrong—and in a cloud computing model, when things go wrong they may be outside the user's immediate control.

The second principle of effective cloud security is to ensure that the legal relationship between company and its cloud provider covers the company for the cloud service's failure. Companies should ensure that the contract allows them to hold the cloud provider accountable for security failures caused by their errors.

Many contracts with cloud operators have a hold-harmless clause within the contract that favors the cloud operator. This runs counter to what companies should expect, since it places all of the costs on the company, without providing the company the ability to control the circumstances.

If a cloud computing provider insists on such a provision, companies should seriously consider other options.

On the other hand, from the cloud providers' perspective (and their professional liability

underwriters!), they need to obtain as much indemnity as they can, as a single error or omission might affect a large number of customers.

A balancing act must be performed to make sure neither side is taking excessive risk. The fairest result is probably a "cross-indemnification" provision under which each side takes responsibility for losses resulting from its own errors or omissions.

Another key part of the contractual analysis is ensuring that the cloud provider has appropriate errors & omission insurance that will cover the company's costs if a breach occurs. The coverage amount should be appropriate to not only cover the company's loss but the cloud provider's other customers' losses as well.

As noted above, part of the issue with cloud computing is that a failure of security will likely affect numerous customers simultaneously. Making sure that a provider is responsible for its actions is part of a larger principle of cloud security, namely vendor selection and management.

Organizations must remember that these providers and their employees will have access to data and be responsible for making the data available and secure. It is critical that companies develop an understanding of the cloud providers before they hand this data over to them.

Companies need to know about the cloud provider they are selecting. How long has it been providing cloud-based services?

A company doesn't want the cloud provider to be learning with its account and its data.

What is its financial situation? A cloud provider that is struggling financially will more likely take shortcuts that put a company's data at risk than one which has adequate resources.

What vendors does the cloud provider use and how do those vendors affect the company using cloud services? If a cloud provider is relying on a managed security firm, a company should know that and do due diligence on the managed security firm.

Many cloud providers rent space in larger data centers, which is something that can affect the cloud company's client's security.

What kinds of audits or assessments has the cloud provider undergone? Companies want to know they not only enact security properly but that they are having that verified with outside parties.

One of the keys to the vendor management principle is continuous monitoring. While it is important to undergo good vendor selection, companies should not forget to reevaluate these concerns on a regular basis. If a cloud vendor's financial condition deteriorates, a company wants to know. If they fail an audit, that should be known as soon as possible.

Companies should make vendor management of their cloud providers a continuous process with reviews at least annually, but more often if possible.

E&O INSURANCE BASICS

The final principle of good cloud security is to transfer some of the risk a company takes to a third party. Even though companies should be holding cloud computing providers liable for their actions, frequently the liability coverage they provide is not enough to cover all costs associated with the breach. Moreover, not all security breaches in the cloud are the fault of the cloud provider. Just because data is breached in the cloud does not mean the cloud provider was at fault, or that its insurance will respond.

For example, the use of poor passwords to protect a company's data is not the fault of the provider nor are actions taken by a company's rogue employee. In these cases, companies need coverage of their own.

Businesses using cloud models—and their agents—should make sure that their insurance coverage will respond regardless of whether the security breach occurs on their own systems, or “in the cloud.” For example, when evaluating network security and privacy insurance, companies need to secure coverage broad enough to apply to personal data maintained by others on the insured's behalf.

Appropriate coverage should include notification costs to inform customers of a breach, reputation

repair coverage that will provide resources to help with the public relations, credit monitoring costs that will provide end customers with credit monitoring services, and cyber extortion coverage that will pay ransoms if a system is taken over by an extortionist. If a company applies these principles of good cloud computing security, it will be in a much better position to utilize cloud computing as part of its overall IT infrastructure.

It is very difficult, especially for small and medium-sized business, to operate without cloud services, and so the key is appropriate risk management of those services, not necessarily avoidance. Failure to manage it appropriately will either put a company at more risk than they want or close the door to services that would otherwise improve their technology environment.

Erich Bublitz is the Technology Practice Leader at ThinkRisk Underwriting Agency, a managing general underwriter in Kansas City, MO, specializing in media, technology and network security risks. He may be reached at ebublitz@thinkriskins.com.

SECURITY PRINCIPLES

Companies that use cloud service providers should: Remember that they are responsible to their customers, not their cloud providers.

Ensure that the contract allows them to hold the provider accountable for security failures caused by their errors.

Ensure the cloud provider has enough errors & omission insurance to cover company's costs if a breach occurs, as well as losses of other customers.

Know their selected cloud provider, asking questions about how long they've offered services, what their financial situation is and what vendors they use.

Make vendor management of cloud providers a continuous process.

Transfer some risk to a third-party insurer, since the cloud providers liability coverage may be insufficient to cover all costs associated with a breach.

HOUSTON AUTO BODY ASSOCIATION

ACRA has been following the Houston Auto Body Association's complaint to and subsequent survey by the Texas Department of Insurance. TDI sent to insurance companies a questionnaire, styled more like a discovery document, and the insurance companies responded. HABA requested a copy of the responses and this was denied, pending a review of Texas FOI law by the Texas AG. TDI eventually did release to HABA a copy of the responses, which I have received. The document is 154 pages long and I am still trying to digest and reduce the information at publishing time. I hope to have highlights and/or summary in the next newsletter. - Jay Scott

OCTOBER 2010 CONSUMER REPORT MAGAZINE

I have been informed the October 2010 edition of Consumer Report Magazine has an article entitled: ARE LOW-COST REPLACEMENT BUMPERS SAFE? This may be an article of interest to our members. ACRA does not have permission at this time to reprint the article.

2010 EDUCATIONAL PROGRAMS:

January 12, 2010	Educational Program by Pulaski Tech Collision Repair Dept.
February 9, 2010	cancelled due to SNOW!!
March 9, 2010	Landers Toyota on current recall issues
April 13, 2010	AllData
May 11, 2010	Red Ball Oxygen on welding issues
June 2010	I-CAR Class – Contact Jody Gatchell
July 13, 2010	LKQ Corp – after market and salvaged parts
August 10, 2010	Freda Keller, Farmers Insurance – Shop Safety/Workers Compensation
September 14, 2010	GM Parts Program by Dana Haswell
October 12, 2010	6H Rule by ADEQ
November 9, 2010	I-CAR Certification Update
December 2010	– there will be no meeting.

ACRA meets the second Tuesday of each month at 6:00 PM at the new Pulaski Technical College campus, 13,000 Interstate 30, Little Rock, Arkansas. The meeting is an open meeting with meal served at 6:00 PM and Educational Program immediately following. If there is a program or topic that you would like presented as an ACRA Educational Program please contact Jay Scott at (501) 351-0171.

ACRA OFFICERS

President	Jody Gatchell, Little Rock	jody@ajcollisionrepair.com
Vice President	Larry Golden, Little Rock	larry@goldencollisioncenter.com
Treasurer	Adam Reiter, Hot Springs	adamreiter@cablelynx.com
Members at Large:	C.J. Bell, Des Arc	carbell@centurytel.net
	Phil Plyler, Little Rock	rivercityauto@sbcgrbal.net
	Kevin Strayhorn, Little Rock	kdstrayhorn@gmail.com

ACRA Sponsors:



CALL PREFERRED AT 401-327-7024



2010 ACRA MEMBERSHIP DUES

2010 ACRA Membership Fee is DUE NOW. Please support your Collision Repair Association by mailing you Membership Fee of \$150.00 to ACRA, 109 Airway Drive, Hot Springs, AR 71913.

Name of Collision Repair Member: _____

Address: _____

Office Telephone: _____

FAX Telephone: _____

Web Site: _____

E-mail Address: _____

ACRA
826 North Creek Circle
Conway, AR 72032