

The cost of piracy

The U.S. automotive industry is probably losing billions of dollars a year to product piracy. Since counterfeiting is illegal, there are no sales reports showing actual dollar amounts, but the bottom line is that the fake parts business is a very costly fact of life.

"This problem is not going to go away," said Mahesh Lunani, Partner at **Roland Berger Strategy Consultants**. The consulting firm's 2004 study, "Intellectual Property Protection in China," underscores a pervasive problem that automotive suppliers and vehicle makers are encountering.

Counterfeit components produced in China are popping up in Africa, Europe, South America, and North America. The fake aftermarket parts are "visually very similar to the real product, and the quality of the packaging has improved—virtually no more misspellings or wrong addresses," said Scott Emmer, Brand Protection Manager for **Federal-Mogul**.

The country posing the biggest piracy-related headaches is also the country predicted to have the biggest automotive sales gain in the coming years. "By far, China is the biggest infringer out there," said Emmer. North America's largest association for automotive and truck parts makers, the **Motor & Equipment Manufacturers Association**, notes that fake parts are also coming from other emerging markets such as Brazil, India, Taiwan, Turkey, Malaysia, and Russia.

Even though Emmer is focused on anti-counterfeiting initiatives for products like spark plugs, wiper blades, gaskets, lighting as well as engine and chassis components, the Federal-Mogul official knows that engineering efforts suffer a fallout from counterfeiting tactics. "In a general sense, it stifles innovation," said Emmer, who points out that many companies in the automotive industry must fight counterfeiting and that requires money. At times, cash for protecting intellectual property comes from research and development budgets.

For example, **X-Rite**, a producer of color measurement instrumentation and software, usually invests 10 to 14% of its annual sales into research and development efforts, with a portion of that going toward intellectual property initiatives.

"We want to protect our investments in the future," said Shannon Gary, Category Director of the Industrial Group for X-Rite.

To illustrate that point, the company's X-Rite Color Master version 7.0 software—for assessing color control and formulation data in automotive and other manufacturing environments—has a protective mechanism in place. "Once you patent something, it can be disclosed to the public," Gary said, referencing why the patent addresses the usage process because that "represents a stronger intellectual property position than patenting the algorithms."

Like many companies, **Delphi's** name is vested in the technical attributes of its products. "We're very diligent about data and product security," said Delphi Vice Chairman David Wohleen. The company has had a presence in China since 1993, and its manufacturing ventures produce more than 40 products, including wiring harnesses, batteries, drum brakes, and automotive electronics.

In the fall of 2005, Delphi opened a technical center in Shanghai to provide an additional outlet for engineering and product development. But regardless of where product development occurs, the safety of the company's intellectual property remains a big concern. "It's an issue," said Wohleen, adding, "We're a target for having our technology utilized or shared inappropriately."

Doug Halliday, Director of Product Development for **AutoWeb Communications**, a global provider of engineering data exchange services, agrees that intellectual property crime is a major threat to the automotive industry. One of the more insidious crimes is infor-

mation stealing. Even though there is an obvious danger to transmitting data over unsecured networks, not all companies are dispersing information that way.

"There are still too many people using physical media (*i.e.*, tapes and CDs) to exchange data, and that's highly risky," said Halliday, noting that a CD could be lost, stolen, or copied.

Should the information contained on the CD need to go a great distance—such as U.S. to China—there is also a time delay vs. sending the data over a secure network. Halliday cautions that engineering information should be provided on a need-to-know basis. "Share only what's required," said Halliday.

AutoWeb has realized an 1882% increase in its Asia-Pacific business since 2003. "A lot of that has followed the automotive industry's growth into that part of the world. There's a lot of movement of sourcing to the region," said Halliday.

At present, AutoWeb is providing secure data-exchange services to more than 19,000 users at 2500 companies, including **DaimlerChrysler**, **Ford**, and **General Motors**. Before joining AutoWeb, Halliday was Director of the Global Enterprise Collaboration for General Motors, which included responsibility for global data sharing among the company's groups, suppliers, joint ventures, and alliances to support GM's product development activities.

"I can tell you from my previous work experience that you have to be able to do things globally," said Halliday. He knows that more companies will realize the importance of having a secure means of protecting engineering and product development data. Otherwise, those companies could be among next year's grim statistics for having monetary and information losses attributed to piracy.

Kami Buchholz

Officials conduct a seizure of a facility in China that was producing counterfeit air filters.

