Next-Level Glass

By Dave Cooper

The evolution of the central part of windows, namely the part you can see through, is well known. And a crawling evolution of improved performance is reflected in the Energy Star requirements as well as in building codes. But is a slow clock-speed inherent to the glass industry?

It's worth noting that when the government passed the so-called .30/.30 performance requirements for tax credits in 2009, glass manufacturers rapidly developed and launched new low-E coated glass products at a breakneck pace to meet those demands. This proved that rapid advancement can be achieved in our industry given proper incentive.

The factors determining overall thermal performance of windows as it relates to Energy Star is a balancing act between insulating glass (IG) and thermal performance of frames. For this reason, window manufactures often specify IG to achieve the overall window U-factor desired.

But how good can we get with IG? Current mass-produced IG performance pushes R-8 center of glass measurements with triple pane, high performance low-E coating(s) and a Krypton gas fill. Low-E coatings are tuned for solar heat gain properties. Further enhancement is possible with even more lites or occasionally, transparent films in the cavity. The current target is mass-produced R010 windows, as put forth by the Department of Energy's Building Technology Office roadmap.

Currently, a thin-triple concept promoted and patented by Lawrence Berkley National Laboratory (LBNL) is seen as a stopgap that allows window manufacturers to adopt a higher performance R-8 glass package compatible with current frame designs, since it is about ¾-inch thick, like a typical dual-pane IG. There is one drawback to thin-triple designs, however: the center lite is 1 to 2 mm thick, which is not a typical soda-lime glass product and presents handling challenges during fabrication.

Focusing on the IG thermal performance, what is the next-step change?

Going Next Level

Available now, vacuum insulting glass (VIG) manufacturers can achieve R-15 center of glass with tempered VIG products. Other products on the horizon include IG filled with aerogel-type materials which have super low conductivity and take the place of a gas fill. In those cases, performance is predicted to reach R-10 for a ½ - inch cavity fill.

The technologies mentioned push window performance to a whole new level. Of course, there is always the question of cost. These step-change products are still somewhat in the early stage with limited volume. It is likely that the cost for the new IG technology will follow the current cost versus performance curve, which is roughly one dollar per R-value per square foot for established products and technologies. For example, R-1 clear glass is roughly a dollar per square foot, whereas a high-volume triple-pane IG at R-8 is in the $8-per-square-foot range. Once greater adoption takes place, such as with the VIG, demand will create opportunities for more factories, which will help to bring down costs through volume and efficiencies. Soon Energy Star and building codes can reassess their goals for windows and doors, adding much greater thermal efficiency.

Wreaths of Honor

By Doug Carroll

The Wreaths Across America program remembers fallen U.S. veterans, honors active service members and teaches the value of freedom.

Every December, participants lay donated wreaths on the headstones of veterans. Several hardware retailers have made the program a part of their community outreach.

Brownsboro Hardware & Paint, which has two locations in Louisville, Kentucky, sponsored the program for the first time this year after the local chapter of the Daughters of the American Revolution approached the company's new owner Doug Carroll.

"Since we have the Zachary Taylor National Cemetery less than a half-mile from one of our locations, we jumped at the chance to help," Carroll says. "We have always been involved in local, civic and charitable causes, and this is one of the most noble that we have been a part of as a business."

The store matched the first 100 wreaths that customers paid to sponsor.

"We had people walk into the store and sponsor five, 10, 20 and even 100 wreaths, and hundreds more went to our website to sponsor wreaths," Carroll says. "It was really heartwarming to hear our customers' stories of friends or family members who served in the military."

Taylor's Do it Center, which has six locations in Virginia and North Carolina, also participated in the event, accepting donations in the store and allowing customers to round up their purchases as a donation during the month of November. This was the retailer's fifth year participating in the event, says Meg Taylor, communications manager.

"Our family has strong military connections, and we operate in a community with strong military ties. Like our customers, we deeply recognize the importance of our veterans and the ultimate sacrifice that many have made," Taylor says. "We will gather to give thanks with friends and family during the holiday season, and for many military families, there will be an empty seat at the table."

Jeannie Bible, store manager for Big R in Fernley, Nevada, has honored military veterans for many years by placing holiday wreaths on graves at the veterans cemetery in her community. Joining the company as store manager four years ago has allowed her to grow her participation in Wreaths Across America. Under Bible's leadership, Big R's Fernley store contributes products to raffle off for an annual fundraiser that helps raise money to pay for wreaths and support veterans with financial needs.

Bible participates as a contestant in the fundraising event, a poker run that involves contestants driving all-terrain vehicles to collect poker cards. Bible contributes all of her poker winnings to the fundraiser.

In addition, she and employees from the store work every year with other volunteers to place thousands of wreaths on the graves of military veterans.

"It's a great way to give back," Bible says. "Our cemetery is so beautiful."

What really makes a good business relationship?

By: Rick Davis

It's all about the relationship. Every salesperson says it, but probably disagrees about what constitutes a good relationship. Have we really defined, in sales, what makes up a good relationship? Is it friendship? Is it business? Is it both? Does the buyer define a relationship in the same way as the salesperson? Many salespeople say the moment they can call a customer their friend it is the pinnacle of success. I assert that the moment you call a customer a friend, you'd better be careful. We've all seen friendships and families destroyed by bad business relationships, proving that friendship can be a byproduct of a good business relationship, but not the foundation for it.

Friends expect favors and invite you over for social interactions while asking you to bring your tool kit to fix a problem. Friends expect discounts and preferential treatment. A friend can be a customer, but the two relationships should be treated differently. If your customer is really a friend, they pay you for your services fairly although I often recommend charging friends more. The inevitable, casual request to fix a problem is really a $300 repair call they want discounted to a price of a cold beer.

If it isn't friendship, then what is a good "relationship"? Many salespeople argue that business comes first and that the best price for service and value is the differentiator. However, hardly anyone would agree that the lowest price is the key to a good relationship.

Many salespeople rationalize that a good price will get your foot in the door and set the stage for a good relationship down the road while leaving unanswered the definition of a good relationship. Ultimately, the definition of a good business relationship must be tangible or else there is no use bragging about it, and everyone else can continue to claim it. (I've yet to see a salesperson say the key to their success is a bad relationship!)

Author and presenter Robert Cialdini, in his landmark book, *Influence; The psychology of Persuasion,* was onto something directly to relationships. In his studies, he provided a clinical analysis for six factors of influence, including "liking," "authority," and "social proof." Importantly, these are not instinctive factors of sway but, instead, intentional actions necessary to create it.

Liking, he notes, is accomplished with sincere praise and intentional discovery of commonality, preferably in professional realm such as a referral, a networking group, or shared project success. The same can be said about authority, which he cites requires credibility based on trust and knowledge. In other words, you can't assume others believe in your competence and authority, you must promote or demonstrate your credentials to them.

This leads to the importance of another factor for influence, social proof, such as the testimonials of other people. Cialdini conducted his research decades ago, before the internet boom. Thus, I find social proof to be one of the most important factors of sway towards a successful relationship. The things you say about yourself in the age of Yelp and Google reviews are not nearly as important as the things other say about you.

The conclusion I draw about the subject of relationships is very simple. The business relationship is established when the seller intentionally discovers commonality and achieve the buyer's goals. The relationship is successful when the seller helps the buyer succeed, the buyer knows it, and happily tells others. Okay, so you might not get the testimonial from everyone, but you get the idea. It's not enough to say you can't define a good relationship, but you know it when you see it. It's essential to define it so you can pursue it with intention.

Doubling – Down on Ransomware Protection

By: Joe Dysart

As the threat of ransomware has reached new heights in 2021, many lumber and building materials business are doubling-down on their defense against the scourge – making sure they've done everything they can to avoid becoming a victim.

"This year, we've already received 13 cyber claims – all of which were either the result of ransomware or spoof mail," says John Smith, president and CEO of Pennsylvania Lumbermens Mutual Insurance Company.

Many owners of even the smallest lumber and building materials business realize they are prime targets for these hackers, who see small businesses as generally easy to penetrate, plunder and fool.

"Ransomware is most commonly known to spread through a malicious link via phishing email. And that's probably where most perceive the risk, "Smith says. "But the web is the next most common way to spread ransomware. We Google everything and point-and-click away, not thinking much about the validity of the content until after we've already clicked."

Indeed, successful ransomware attacks across the U.S. have proven so visceral this year, they triggered an executive order from President Joe Biden – urging all U.S. businesses to get serious about ransomware protection. Biden's order "calls for federal agencies to work more closely with the private sector to share information, strengthen cyber security practices, and deploy technologies that increase reliance against cyberattacks. It outlines innovative ways the government will drive to deliver security and software – using federal buying power to jumpstart the market and improve the products that all Americans use."

During 2021 alone, businesses across the U.S. have been reeling from successful ransomware disruption of service on the Colonial Pipeline, the largest conduit of refined oil products in the U.S. and the ransomware seizure of computer files of the Washington DC Metropolitan Police Department.

Still other ransomware takedowns include a takeover of computer files at goliath meatpacking concern JBS Foods as well as the National Basketball Association.

Granted, authorities have occasionally gotten lucky against ransomware hackers during 2021. Excellent cyber forensic work by the U.S. Department of Justice, for example, clawed back $2.3 in Bitcoin that the Colonial Pipeline paid to ransomware hackers to help get its computer network up-and-running again.

"Following the money remains one of the most basic, yet powerful tools we have. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks. Today's announcements also demonstrate the value of early notification to law enforcement. We thank Colonial Pipeline for quickly notifying the FBI when they learned that they were targeted by Dark Side," said Lisa O. Monaco, US deputy attorney general. Even so, hackers more often than not get away with their exploits, extorting hundreds of thousands of businesses across the globe each year – and disrupting the day-to-day operations of each. Overall, 37% of organizations across the world have experienced some sort of ransomware attack between May 2020 to April 2021, according to a study from cybersecurity firm Sophos.

Based on that survey of 5,400 IT managers at mid-sized organizations across 30 countries, the study also found that the average ransom paid to recover data from a ransomware attack was $170,404.00. Not surprisingly, many of the criminals behind those successful ransomware attacks ignored promises to restore computer files once ransoms were paid, according to the study.

Specifically, on average, victimized organizations in the study that paid ransoms only received 65% of their data. And only 8% of organizations forking over money to hackers were able to retrieve all their files, according to the Sophos study. Equally vexing for the victim organizations was the cost to day-to-day business. On average, the cost to restore the impact of a successful ransomware attack on a mid-size business – taking into account downtime, lost wages, device cost, network cost, lost sales, and ransomware paid was $185 million.

Plus, hackers have increasingly exploited a new wrinkle in their ransomware schemes during the past year – threatening and often making good on threats – to publish sensitive data found in business files on the Dark Web if a victim business refuses to pay a ransom.

While news stories tend to focus on ransomware attacks on large corporations, LBM businesses are just as likely to be targeted by hackers. Plus, even at the smallest lumber and building materials business, a ransomware shutdown hurts, grinding its revenue stream to a halt and running the owner ragged trying to find a way to get computers up-and-running again.

That's why it's imperative to start putting together a plan, you'll most likely be caught flatfooted, struggling to deal with a swirl of chaos that might force you to make quick decisions you'll later regret. "For example, our cyber security incident response plan empowers the head of IT and our cyber partner to shut down systems immediately if it is deemed necessary to contain or research a serious event such as a ransomware attack, "Smith said. "You often can't think those kinds of things in the moment."

But perhaps most important in safeguarding your lumber and materials business against a hacker breach is ensuring your employees are brought up-to-speed on all the ways hackers are trying to trick them into clicking on links, revealing IDs and or passwords or otherwise providing access to the company network that can, and often does, result in devastation.

"The human factor is the most concerning to us when it comes to ransomware. Be sure you engage your entire company and build a cyber-aware culture. Have a plan in place to educate your staff on what to look for and how to report suspicious emails or links," Smith said.

In the end, it appears the scourge of ransomware and similar cybersecurity threats is doomed to relentlessly playout as a never-ending game of cat-and-mouse.