

▶ INTRODUCING SECURITY SOLUTIONS 1

▶ Food Retailers Making a Dent in Shrink Rate 1

▶ Corporate Security Weak Link: Old Cell Phones? 2

▶ The Low Light Revolution 4

▶ Christmas Security 6

○ ISSUE
1

○ VOLUME
1

○ December
2006

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

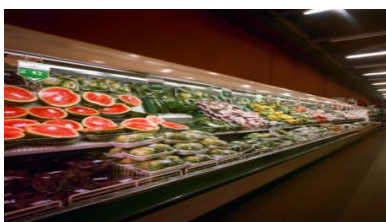
Crime and its effects impacts everyone at all levels of society. There is a heightened degree of concern as people search for solutions to protecting their home, business, employees and families. Amalgamated Security Services as one of the region's leading security companies recognizes the extent of concern and the search for answers along with its role in helping provide solutions to security issues. To that end, Amalgamated Security now launches **SECURITY SOLUTIONS**, a bi-monthly newsletter aimed at providing solutions to security issues.

The continuing development of technology along with the integration of that technology is providing a steady stream of solutions to what were once intractable security problems.

Over the coming months we will provide articles that focus on security problems and methods to resolve those problems. While there will be a mix of articles, the bias will be towards security technology.

If any additional persons in your organization would like to receive this email newsletter just send an email to newsletter@assl.com with the words "Subscribe Newsletter" in the subject line. To opt out of the mailing list send an email with the words "Unsubscribe Newsletter".

Brian Ramsey
Editor



Food Retailers Making a Dent in Shrink Rate

Food retailers used technology, surveillance, hotlines, and other tactics to decrease losses from theft and other forms of shrink to 1.69 percent of sales in 2005, down from 2 percent the previous year, according to the Food Marketing Institute's Supermarket Security and Loss Prevention 2006 report.



Food Retailers Making a Dent in Shrink Rate

New frauds striking businesses, but food retailers aim back with technology

their bottom line is lower because they recover more losses and prevent more crime."

Shrink among the top performers was a median of 0.67 percent of sales in 2005, the report found. The most common methods to prevent theft in 2005 included:

*Closed-circuit television (CCTV), used by 97 percent of the retailers surveyed.

*Monitoring point-of-sale transactions, used by 76 percent.

*Employee hotlines, used by 70 percent.

*Biometric readers used in store check cashing, door entry, time clocks, and customer payments, employed by 23 percent.

"Retailers who reduce shrink are the most vigilant and foster a culture of low tolerance," observes FMI s.v.p. Michael Sansolo. "They detect more theft, worthless checks, counterfeit money, and fraud, yet the impact on

Employee theft, shoplifting, and organized retail crime (ORC) ranked as the top three most serious causes of losses. ORC in particular is a growing problem, notes FMI. Over 60 percent of the retailers surveyed reported an increase in this method. Many large retailers have loss prevention units focusing exclusively on organized retail crime.

Nearly 40 percent of all shrink was attributed to stealing by store employees in 2005, averaging 4.3 cases per store -- a figure that has remained stable over the past five years. Losses from employee theft averaged \$467 per store and \$235 per incident. The cash register and service departments continue to be the most vulnerable, accounting for 62 percent of employee theft.

Retailers apprehended nearly one shoplifter per company per day in 2005, averaging 16 per store and \$29.62 per incident. The most frequently stolen items

were meat, over-the-counter medicines, health and beauty care products, razor blades, and baby formula.

Robberies and bad checks remain a costly problem for retailers as well. Six in 10 companies reported at least one robbery, costing retailers an average of \$3,543 per incident. Supermarkets accepted more than a half-million worthless checks, resulting in a median loss of \$57,567 per company in 2005.

A new form of fraud has surfaced as gift cards have grown in popularity. Criminals tamper with bar codes to increase the value on stolen cards and buy gift cards with worthless checks or stolen credit cards, effectively laundering them. Two-thirds of retailers selling gift cards experienced some form of tampering, fraud, or theft. Ψ

Reprinted from **Progressive Grocer**

SMARTER SECURITY:
Experience & Discipline



Amalgamated Security provides a full range of security services, which include:

**Cash Services
Electronic Security
Access Control
Data Storage
Courier Services
Guarding Services
Alarm Monitoring
Response Services**

Corporate Security Weak Link: Old Cell Phones?

Don't tell your cell phone any secrets. It might not keep them.

Second-hand phones purchased over the Internet surrendered credit card numbers, banking passwords, business secrets and even evidence of adultery.

One married man's girlfriend sent a text message to his cell phone: His wife was getting suspicious.

Perhaps they should cool it for a few days.

"So," she wrote, "I'll talk to u next week."

"You want a break from me? Then fine," he wrote back.

Later, the married man bought a new phone. He sold his old one on eBay for \$290.

The guys who bought it now know his secret.

The married man had followed the directions in his phone's manual to erase all his information, including lurid exchanges with his lover. But it wasn't enough.

Selling your old phone once you upgrade to a fancier model can be like handing over your diaries. All sorts of sensitive information pile up inside our cell phones, and deleting it may be more difficult than you think.

A popular practice among sellers, resetting the phone, often means sensitive information appears to have been erased. But it can be resurrected using specialized yet inexpensive software found on the Internet.

A company, Trust Digital of McLean, Va., bought 10 different phones on eBay this summer to test phone-security tools it sells for businesses.

The phones all were fairly sophisticated models capable of

working with corporate e-mail systems.

Curious software experts at Trust Digital resurrected information on nearly all the used phones, including the racy exchanges between guarded lovers.

The other phones contained:

_One company's plans to win a multimillion-dollar federal transportation contract.

_E-mails about another firm's \$50,000 payment for a software license.

_Bank accounts and passwords.

_Details of prescriptions and receipts for one worker's utility payments.

The recovered information was equal to 27,000 pages - a stack of printouts 8 feet high.

"We found just a mountain of personal and corporate data," said Nick Magliato, Trust Digital's chief executive.

Many of the phones were owned personally by the sellers but crammed with sensitive corporate information, underscoring the blurring of work and home. "They don't come with a warning label that says, 'Be careful.' The data on these phones is very important," Magliato said.

One phone surrendered the secrets of a chief executive at a small technology company in Silicon Valley. It included details of a pending deal with Adobe Systems Inc., and e-mail proposals from a potential Japanese partner:

"If we want to be exclusive distributor in Japan, what kind of business terms you want?" asked the executive in Japan.

Trust Digital surmised that the U.S. chief executive gave his old phone to a former roommate, who used it briefly then sold it for \$400 on eBay.

Researchers found e-mails covering different periods for both men, who used the same address until recently.

Experts said giving away an old phone is commonplace. Consumers upgrade their cell phones on average about every 18 months.

"Most people toss their phones after they're done; a lot of them give their old phones to family members or friends," said Miro Kazakoff, a researcher at Compete Inc. of Boston who follows mobile phone sales and trends. He said selling a used phone - which sometimes can fetch hundreds of dollars - is increasingly popular.

The 10 phones Trust Digital studied represented popular models from leading manufacturers. All the phones stored information on "flash" memory chips, the same technology found in digital cameras and some music players.

Flash memory is inexpensive and durable. But it is slow to erase information in ways that make it impossible to recover. So manufacturers compensate with methods that erase data less completely but don't make a phone seem sluggish.

Phone manufacturers usually provide instructions for safely deleting a customer's information, but it's not always convenient or easy to find.

Research in Motion Ltd. has built into newer Blackberry phones an easy-to-use wipe program.

Palm Inc., which makes the popular Treo phones, puts directions deep within its Web site for what it calls a "zero out reset." It involves holding down three buttons simultaneously while pressing a fourth tiny button on the back of the phone.

But it's so awkward to do that even Palm says it may take two people. A Palm executive, Joe Fabris, said the company made the process deliberately clumsy because it doesn't want customers accidentally erasing their information.

Trust Digital resurrected erased e-mails and other information from a used Treo phone provided by The Associated Press for a demonstration after it was reset and appeared empty.



Once the phone was reset using Palm's awkward "zero-out" technique, no information could be recovered. The AP already used that technique to protect data on its reporters' phones.

"The tools are out there" for hackers and thieves to rummage through deleted data on used phones, Trust Digital's chief technology officer, Norm Laudermitch, said. "It definitely does not take a Ph.D."

Fabris, Palm's director of wireless solutions, said after AP's inquiries that the company may warn customers in an upcoming newsletter about the risks of selling their used phones. "It might behoove us to raise this issue," Fabris said.

Dean Olmstead of Fresno, Calif., sold his Treo phone on eBay after using it six months. He didn't know about Palm's instructions to delete safely all his personal information. Now, he's worried.

"I probably should have done that," Olmstead said. "Folks need to know this. I'm hoping my phone goes to a nice person."

Guy Martin of Albuquerque, N.M., wasn't as concerned someone will snoop on his secrets. He also sold his Treo phone on eBay and didn't delete his information completely.

"I'm not that kind of valuable person, so I'm not really worried," said Martin, who runs the <http://www.imusteat.com> Web site. "I guarantee that three-quarters of the people who buy these phones don't think about this."

Trust Digital found no evidence that thieves or corporate spies are routinely buying used phones to mine them for secrets, Magliato said. "I don't think the bad guys have figured this out yet."

President Bush's former cybersecurity adviser, Howard Schmidt, carried up to four phones and e-mail devices - and said he was always careful with them. To sanitize his older Blackberry devices, Schmidt would deliberately type his password incorrectly 11 times, which caused data on them to self-destruct.

"People are just not aware how much they're exposing themselves," Schmidt said. "This is more than something you pick up and talk on. This is your identity. There are people really looking to exploit this."

Executives at Trust Digital agreed to review with AP the information extracted from the used phones on the condition AP would not identify the sellers or their employers.

They also showed AP receipts from the Internet auctions in which they bought the 10 phones over the summer for prices between \$192 and \$400 each.

Trust Digital said it intends to return all the phones to their original owners, and said it kept the recovered personal information on a single computer under lock and disconnected from its corporate network at its headquarters in northern Virginia.

Peiter "Mudge" Zatkó, a respected computer security expert, said phone owners should decide whether to auction their used equipment for a few hundred dollars - and risk revealing their secrets - or effectively toss their old phones under a large truck to dispose of them.

What about a case like the Lothario whose affair Trust Digital discovered?

"I'd run over the phone," Zatkó said. "Maybe give it an acid bath." Ψ

By TED BRIDIS
Associated Press Writer

The Low Light Revolution

Charlie R. Pierce

One of the biggest problems with camera systems has always been producing viable, working images in the dark. I'm not just talking about low light, I mean in the dark. Yes, we have had the technology to look around in the dark for the past 30 years, but could we afford it, and could we do it in color? Let's start with a quick overview of the problems that face image production in the dark.

In the Dark

The first step is to understand how a camera sees. It produces an image the same way the human eye does. We take the reflective light from a scene and focus it on the imager, which is made up of several light-sensitive points (pixels). The imager creates an electronic pattern in response to the highlights and colors. Simple.

The first mistake most designers make is measuring the ambient light in an area and considering that measurement to represent the light the camera uses. However, cameras see reflective light as well, so with only an ambient light measurement, we come up anywhere from five percent to 95 percent short in our lighting. For example; if the ambient light at the darkest point in a parking lot is .01 foot candle (fc), we must remove 95 percent of that

to determine the actual working light of the camera, because asphalt has a five percent reflectivity. The consequence is that we really have .0005 fc of usable light in that parking lot at night.

Light loss caused by the lens is another impact that may be missed. Light loss from the lens can be as much as two to three f-stops. An f-stop is a unit of measurement assigned to light gain or loss. One f-stop gain is equivalent to a 50 percent decrease in light, and one f-stop down is equal to a 100 percent gain in light. Therefore, if our lens has a two f-stop light loss factor, we must decrease our .0005 fc by 50 percent two times (once for each f-stop): $.0005 \text{ fc} / 2 = .00025 \text{ fc} / 2 = .000125 \text{ fc}$. Now we don't have to know what a fc of light is to be able to understand that there is a huge difference between the original ambient light measurement of .01 fc and the final .000125 fc.

Our dilemma lies in the lack of useable reflective light for the camera and the lack of color reflectivity below 2 fc of ambient light.

Options and Pricing

A short five years ago, our options in the above situation were limited. We had four choices:

- 1) Use a black /white (BW) camera with good sensitivity.
- 2) Use an intensified camera (also BW)
- 3) Use an infrared enhanced lighting scheme with an IR-sensitive camera (also BW)
- 4) Use a thermal camera (no color orientation).

Five years ago, the sensitivity range for a BW camera directly corresponded with the price. The higher the sensitivity, the higher the cost of the unit. But BW cameras were still the most affordable cameras, ranging from \$800 to \$1,200 for up to .0001 fc. The intensified camera of the past averaged between \$8,000 and \$12,000 without housing or lens and averaged a sensitivity of .00002 fc (half moonlight).

The IR-enhancement light scheme would include one or two large, expensive IR lamps with a potentially expensive camera. As a set, the average IR lamp/camera would cost about \$3,000 to \$5,000 complete.

The thermal camera of five years ago started at around \$50,000 and could work up to \$300,000 very quickly (dependant upon lens and image enhancements). The sensitivity of the IR-enhanced and thermal cameras is a moot point, because the IR camera uses IR light enhancement as an aid and the thermal camera does not recognize light.

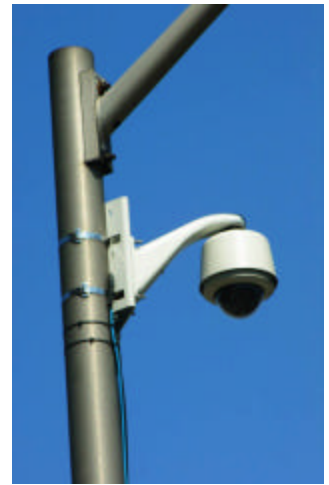
What's New?

So what's so exciting about the market today as opposed to just a few short years ago? Everything!

Color at night. We are quickly realizing color at night. The new color cameras are toting sensitivity ranges as low as .003 fc. This is a huge improvement over the sensitivity of previous versions, and it is literally changing many, if not most of our night views. The door to color at night is wide open and applications are streaming in.

Day/night cameras. The next most exciting step forward are the day/night cameras-color by day, BW by night. They work on three principals.

- 1) Double imagers: A color imager that creates an image until the video signal output drops below an accepted point and then automatically switches over to a more sensitive BW imager.
- 2) Double scan imaging: A color imager that drops out the color portion of the image when the output falls below an accepted level.
- 3) Mechanical IR cut filters: The IR cut filter ensures that the color balance of the image will remain true without being affected by the upper ranges of red or heat in full-light situations. By using a mechanical device to remove the filter from in front of the imager in lower light levels, the color CCD can gain significant improvement in



sensitivity, partially because of the removal of the filter (up to 1 f-stop) and partially because of the enhanced IR sensitivity without the filter.

These bad boys and girls of the day/night group tote an average sensitivity range of .0001 fc. There are two problems, however, that have presented themselves.

The first is related directly to lighting. Some units have a problem switching into the night mode if there are street lamps in the image. This is due to the spike in the video signal that is caused by the intensive point of light from the lamps. The apparent problem is that the electronics of the camera are not designed to quell such spikes and so the unit thinks that it's still daytime.

The second problem comes in the form of white balance. White light is made of equal levels of all colors-red, orange, yellow, green, blue, indigo and violet.

The white balance circuit is designed to make sure that colors stay true by measuring the incoming light against a true white source that is built into the camera and then adjusting the final image against impurities. Since these cameras are so sensitive there are a few models that appear to be having problems with their white balance circuits in the lower light levels. That is, cold lights (florescent) tend to turn the images blue, while warm lights (tungsten) tend to turn the images yellow. It is a problem that can only be solved by replacing the camera, model and all. The best suggestion is to test and demo on site for a day or two. Overall, the day/night cameras range from \$800 to \$1,500 and are proving to be an extremely valuable asset to the design process.

Night vision cameras. New to the market are night vision cameras. These new intensified cameras are bragging and proving an incredible sensitivity of .00000046 fc sensitivity. This is huge and borders on thermal imagery. The best part is that they are affordable within the range of \$6,000 to \$7,000, including housing and lens. Never before have we been able to monitor such a range of areas along perimeters and unlit areas so effectively. For those areas where the light level is just too low, these BW units are able to work with IR lighting enhancements.

I say to these new cameras, welcome to the camera package.

Thermal cameras. Of course, to leave out the thermal camera would be to ignore a viable work horse that is fast becoming a valuable asset to the security design where lighting is just not an option. These cameras work by measuring the temperature of the area of view and then displaying the readings in the form of colors on the screen. Warm objects such as humans will appear in various shades of red, while cold objects are varying shades of blues and blacks. The net result is that these cameras see in sub-zero lighting with no enhancements. The best part is that they can be used for a huge variety of applications, from perimeters to waterfronts.

Yes, they work just fine in full daylight, because they tote visible light filters that block out 100 percent of the visible and IR spectrum. The downfall is that they must use specialized lenses and so are just a little bit restrictive. The best part is that these cameras are more than affordable today, especially when you consider the options and costs involved in increased lighting. Ranging from \$6,500 to \$300,000, these cameras are now to be considered full members of the CCTV industry.

To sum it all up, the night has never been brighter or more affordable. However, I have always promoted and will continue to promote that testing in the field should always be done, whenever and wherever possible, to prove results ahead of investment. Ψ

Reprinted from

Security Technology & Design



Christmas Security

Brian Ramsey

Peace on Earth are the traditional words of Christmas but there are those who would instead take piece of your earth. So amidst the gift buying, cooking and decorating one must continue to maintain vigilance against crime. In this article we provide some security advice for the Christmas season.

- ◆ Avoid carrying too much around with you. The more bags you have the more vulnerable you are to crime. Make regular trips to your car to store your presents - provided your car is parked in a well-lit public place.

- ◆ Make sure all items stored in your car are locked away, well out of sight, and ideally they should be placed in the trunk.
- ◆ If you don't have a car and plan to use public transport, take someone else with you to help carry the load, or try making a number of trips.
- ◆ Keep your purse or wallet somewhere where you can feel it, such as an inside jacket or trouser pocket. Check every so often that you still have your wallet or purse on you. However when checking do not make it too obvious as pickpockets can spot you doing this and so know where your money is hidden.
- ◆ If you need a break from shopping, say for a cup of tea or coffee, don't leave your bags unattended even if it's just for a few seconds.

- ◆ Keep a close eye on your bag when shopping for food. Supermarkets are extra busy at Christmas, making it easy for someone to snatch your bag while you look for something on the shelves or when you're packing your bags at the register.
 - ◆ Keep valuable gifts out of sight inside your home. Under the Christmas tree is one of the first places a burglar will look so do not keep the expensive gifts there.
 - ◆ Keeping gifts under the Christmas tree is all part of the tradition, so if you really want to keep them there make sure the bottom of the tree is situated where no one can see it from outside your home - there's no point tempting a burglar to break-in.
 - ◆ Be extra wary of bogus callers around Christmas time, which could include carol singers or parang groups. Make sure your back door is locked whenever someone is keeping you occupied at the front door.
- ◆ One holiday problem that can occur is the running of exterior Christmas light extension cords from inside the house through a window. This prevents the window from being secured. Hire an electrician or handyman to install an inexpensive exterior outlet for your holiday lights.
 - ◆ After Christmas do not pile up empty gift boxes from your new computer, DVD, stereo etc. out on the street for the garbage truck. These large boxes outside your home advertise to burglars that you have expensive items inside that they can steal. Break down or cut up the boxes before placing for the garbage truck so that the types of items are not easily visible. Ψ

Remember to send your emails to newsletter@assl.com to add individuals to the circulation list