- Editors' Note……..1
- How to reduces losses caused by theft at POS…….....2
- Macros what they are and how they can imperil……..……..4
- How to improve Print Security or a CCTV System……..…….6
- Wide Dynamic Range Camera the best feature for video camera…….....7

Issue 2 | Volume 10 | June 2024

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note:
In this issue of Security Solutions Magazine, we delve into some critical aspects of safeguarding your business, both digitally and physically. From preventing theft at the point of sale to securing your printed documents, we have expert insights to help you stay ahead of potential threats.

Reduce Losses Caused by Theft at Point of Sale
Retail theft remains a significant concern for businesses, impacting profit margins and overall security. We explore effective strategies to mitigate these losses, including employee training, advanced point-of-sale systems, and real-time monitoring solutions. Learn how to create a robust loss prevention plan that not only deters theft but also enhances operational efficiency.

Macros! What They Are and How They Could Imperil You
Macros, while incredibly useful for automating tasks in software like Microsoft Office, also pose a substantial security risk if exploited by cybercriminals. In this article, we break down what macros are, how they work, and the potential dangers they present. Discover best practices for using macros safely and the steps you can take to protect your organization from macro-based attacks.

How to Improve Print Security
Printed documents can be a significant vulnerability if not properly secured. From sensitive financial records to confidential employee information, the data you print needs protection. Our experts share tips on enhancing print security through controlled access, secure printing solutions, and regular audits. Find out how to safeguard your printed information from unauthorized access and breaches.

Wide Dynamic Range Cameras: Enhancing Security Surveillance
Surveillance technology continues to evolve, and wide dynamic range (WDR) cameras are at the forefront of this advancement. WDR cameras offer superior image quality in varying lighting conditions, making them ideal for comprehensive security coverage. This article explains the benefits of WDR technology, its applications in different environments, and how it can significantly improve your security infrastructure.

Stay informed and proactive with the latest strategies and technologies in security. Your commitment to security today ensures a safer, more secure future for your business.

Regards

Carril Reyes-Telesford
Regional Marketing Specialist

How to reduce losses caused by theft at POS

By Bob Violino

Retail theft is a huge and costly problem for the industry. According to the "Global Retail Theft Barometer 2013-2014," released by Checkpoint Systems in October 2014, total shrinkage among retailers in North America was $42 billion for the time period covered by the report.

North American companies had the highest shrinkage rate in the world, "as it has the highest concentration of retail stores and significantly lower retail loss prevention spend" than other regions, the study notes. U.S.-based discounters, pharmacies/drug stores and supermarkets/grocery retailers had the highest shrinkage rates, stemming from shoplifting, dishonest employee theft and organized retail crime.

Nearly all types of retail stores in the U.S. were affected by dishonest employee theft and shoplifting, according to the report.

Retailers can take steps to try to prevent or at least reduce losses due to theft at point of sale (POS) and shrink. Here are some suggestions from experts in the field.

Leverage the latest technologies.

Fortunately for retailers, there's no shortage of technology tools to deter theft and shrink. The use of electronic article surveillance (EAS) technology remains a viable part of retailer's efforts in shrink reduction, says Curtis Baillie, an independent security management consultant specializing in retail security/loss prevention.

This includes using anti-theft tags, spider wraps and technology that detects foil-lined bags and EAS jammers that some shoplifters use to try to bypass surveillance systems, Baillie says. Theft denial systems are also popular with retailers. For example benefit denial systems include ink tags and various other devices such as magnetic stainless steel clips designed to protect neckwear, eyewear and lingerie, he says.

Radio Frequency Identification (RFID) systems, which use tags and readers that enable retailers to track items as they're moved within and outside of a store, can help deter theft and provide information about the type of merchandise that's being taken. Retailers can use EPC tags to identify individual items uniquely.

By combining EAS and RFID systems, retailers can have real-time information about missing items. Dual EAS and RFID tags can provide security as well as inventory visibility, enabling retailers to better track inventory**.**

Other technology tools that can be used to prevent theft are video systems such as closed-circuit television (CCTV), which can be used at the point of sale or elsewhere in stores; and facial recognition systems, which retailers can use to capture images of offenders.

The use of video analytics with overhead CCTV observation of the sales counter "can be a real-time deterrent to incidents of internal shrink," says Bob Moraca, vice president of loss prevention at the National Retail Federation (NRF), the world's largest retail trade association.

"Video analytics is the capability of automatically analyzing video to detect and determine if an anomaly has taken place based on a set of instructions built into the video software," Moraca says. "The technology is able to count items, superimpose the register receipt over the video and then track things like item count compared to the register receipt, voids, returns and even instances where the cash

register drawer has been open too long."

Tracking the variances of these type of irregularities can be an indicator that something might be amiss at the POS and can be followed up with an internal inquiry by management or the loss prevention team, Moraca says.

Train your employees well. The people who work in stores can do a lot to help prevent theft.

"A successful program to reduce shrink at POS leverages both technology and training," says Lisa LaBruno, senior vice president for retail operations at the Retail Industry Leaders Association (RILA), an industry organization.

Among the key components of associate training is making every employee feel like he or she has a responsibility to prevent shrink from occurring," LaBruno says. "Associates are trained to be vigilant, check inside large containers to prevent package stuffing and to exercise good customer service when they suspect theft."

In addition, employees should be encouraged to develop strong product knowledge. "If associates have a strong familiarity with the product they sell and the prices, they are more likely to be able to identify things like UPC [universal product code] switching schemes," LaBruno says.

For some retailers, "many of the loss prevention procedures enacted at the point-of-sale are a result of a more stringent loss prevention program that starts with the hiring process as companies look for qualified candidates for all available positions," Moraca says.

"This also includes offering employee orientation and training opportunities for new hires and even current employees," Moraca says. "For many companies, reminding all employees to keep their eyes open to detect and report potential breakdowns in procedures is a big part of any loss prevention program."

Interact more with customers. In a sort of reverse social engineering tactic, retailers can help stop theft by engaging more with clients while they're in the store.

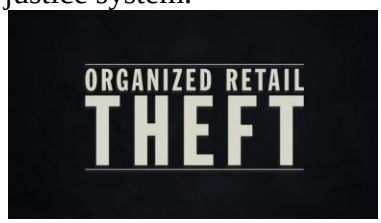
"The most effective deterrent to a potential shoplifter is good customer service, Baillie says. "Making eye contact and acknowledging customers as they enter the store. The last thing a shoplifter wants is interaction with a store employee."

The shoplifter's goal is to enter and exit the store with unpaid for merchandise, without being noticed, Baillie says, and this type of engagement can help work against that.

Consider diversionary tactics. A company called Corrective Education Company (CEC) offers a program to first-time offenders who've been apprehended for shoplifting.

The way the program works, once an offender is apprehended, he is given the opportunity to hear about CEC and the merchant's voluntary education program. The individual's personal information is gathered and verified through public records databases to determine qualification for the program based on retailer protocol, local law enforcement and the local prosecutor.

After agreeing to learn about the program, the offender is shown a four-minute video about CEC's, and can stop the process at any time and not participate. At the conclusion of the video the offender is given the opportunity to participate in a six-hour program, at his own expense, in lieu of having the case referred to the criminal justice system.



If the offender fails to complete the program the retailer has the option to file a criminal

complaint. If the offender doesn't want to participate in the retailer's program or is ineligible due to prior illegal conduct, the matter is referred by the retailer to the criminal justice system, a company spokesman says.

CEC encourages participating retailers to reach out to local law enforcement before implementing the program, in an effort to keep them informed and to gain their support, the company says. Since its inception more than 20,000 participants have gone through the program.

Create the right corporate culture. Anti-theft technologies and tactics are helpful, but they're not enough.

"All the tools in the world are not a replacement for the most critical foundation needed to prevent, isolate and resolve retail losses, and that is a corporate culture focused on mitigating loss," says Keith Aubele, president & CEO of Retail Loss Prevention Group, a consulting firm.

"When a top down ownership/executive C-suite culture exists that truly understands loss impact via shrink to profitability, as well as the many negative societal outcomes from retail crime, then true prevention can occur," Aubele says.

This cultural element "is key, in that once the basic barriers to loss are mitigated by employees who understand the impact of loss through training, awareness, reinforcement, and partnership, it's then that sound tools can be deployed with greater impact," Aubele says. "Essentially, get your house in order first before looking for external help."

Reprinted from Chief Security Officer Online

Macros: What They Are and How They Could Imperil You

Legitimate mini-programs called macros, which run inside other software, are proving to be an increasingly popular route for criminals to hack into victims' computers. Simply put, a macro is a series of commands you can use to speed up or automate tasks in certain popular productivity software like Microsoft Office and Excel. People who know how to use these commands to build a sequence of program actions can save themselves a lot of time and hassle.

But that means crooks can also use them to write malicious macros that run when you try to open an infected document or spreadsheet. They arrive in the form of attachments to emails or as documents on disks, usually with a message that urges you to click on them. Sometimes, they are part of a well-organized campaign such as one spotted in the UK in February this year. In this case, the emails were faked to look

like they were from legitimate companies, and referred to an "attached invoice." But the "invoice" actually contained a macro that would install malware to steal confidential banking information.

One of the Scambusters team members also recently received a similar attempt to install a virus via a macro. In this case, the message appeared as a notification of a failed ACH (Automated Clearing House) banking transaction, which had been rejected by another bank. "Please click the word file given here to get more information about this issue," it said. But the file contained a macro that would have installed a virus known as Trojan Downloader that would then open up a PC to hackers.

In both cases, any attempt to run the macro would likely have encountered the built-in security in Microsoft Word. When this protection is switched on, which it should be by default, a yellow "Security Warning" bar appears in the program, with a shield icon and a button marked "Enable content." So the malicious macro would not run unless you clicked that "Enable" button.

But, unfortunately, as we know, many computer users are simply too trusting and probably would click the button if they thought the message came from a legitimate source. Furthermore, crooks are cunning so, at least in the UK case, the text inside the Word document also contained instructions on how to run macros and bypass the security.

New Threats

Earlier this year, Security Week magazine quoted the Microsoft Malware Protection Center as saying: "Since Microsoft set the default setting to 'Disable all macros with notification,' the number of macro-related malware threats declined. More recently we have seen new threats emerging that include some form of social engineering to convince users to manually enable macros and allow the malicious code to run."

The magazine said the use of malicious macros had spiked during recent months, notably with the use of the fake "ACH Transaction" notification received by the Scambusters team member. Other subject headings include "Invoice as Requested" and "Payment Details." The documents are being distributed as part of a well-orchestrated spam campaign.

So, what can you do to avoid falling victim to malicious macro attacks?

First, check that your software is properly set up to alert you to attempts to run macros. Word and Excel are the most commonly used programs that run macros, though there are others.
To make sure that the macro autorun function is turned off in these two specific applications, see:

https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?CorrelationId=934fca6b-9a6b-4f97-8d28-efff5c7b75d3&ui=en-US&rs=en-US&ad=US&fromAR=1#__toc311698312
Or use this shortcut:
http://bit.ly/1vLaEgV

Second, in these or any other programs that invite you to enable or run macros, be extremely cautious about doing so. If possible, check independently with the supposed sender to authenticate it.

Also be wary about standalone macros available online. In these cases, the macros are not part of another program but independent applications that offer to automate repetitive tasks on your PC. Many of these are free so perform an Internet search on the name to check out others' experiences with them.

Finally, ensure you're running good anti-virus software and keep it up to date. Most security software will spot an attempt to run malicious macros and stop them dead in their tracks.
Reprinted from Scambusters

How to Improve Print Security

By Corey Rogan |

With the security breach of numerous large corporations headlining the news, many companies are focusing heavily on new methods of cyber security in order to safeguard privileged information, both of their own and their clients. In doing so, however, these same companies may be overlooking the importance of print security, or the protection of paper documents that are created by a printer.

In fact, according to statistics provided by Quocirca, a research organization within the European market, over "60 percent of survey participants experienced a print-related breach," whether by unauthorized recipients getting hold of the documents, or even private documents being left uncollected in the printer tray (source: Quocira, "Print Security: The Cost of Complacency").

Overall, print security should be of the utmost importance to all businesses that rely on printed documents. And, to help decrease the possibility of a print-related breach, these companies should employ the following tips to help improve security.

Assess the Security of Printers and MFPs

In reality, many companies have moved beyond basic printers and now use multifunction peripherals (MFPs), machines that act as printers, copiers, scanners, and even faxing devices. In order to perform all of these tasks, however, the devices often have built-in networks, as well as storage capabilities.
To decrease the chance of a print-related breach, companies may wish to utilize the services of a third-party organization to assess the print security, especially if the business uses a significant amount of MFPs that could have vulnerabilities. A security provider can locate specific areas where a breach could occur, and advise on the best way to improve the security of the overall system.

Control and Monitor Access

In addition assessing the security of devices, businesses that utilize printers and MFPs would also be well-advised to control and monitor the access of said machines to ensure that only authorized individuals are eligible for use. Specifically, businesses can take advantage of processes known as PIN or pull printing, whereby printing tasks can be saved either on the MFP or on a separate device. Only by using a PIN code, swipe card, or other security device can the authorized individual can gain access to the print job, keeping it protected from other unauthorized parties.

Find the Right Device

Print-related security breaches can take many forms. For instance, an unauthorized party could snatch a confidential document from a printing tray; or, the same individual could gather private information that was left on the MFP.

To combat this, businesses should consider purchasing a newer set of devices that are manufactured specifically with security in mind. Many printing and MFP devices, such as the security printers, now come with lockable and removable hard drives, as well as locking trays to safeguard paper stock (source: TROY Group, "Security Printers"). Furthermore, these security devices may also erase all data once a separate device is disconnected, and offer built-in hard drive encryption as well.

Focus on Security

Even as society moves further into the digital revolution, many businesses still rely on the use of printed documents to transfer information. And to protect their paper, these companies should utilize the aforementioned tips to improve print security for the benefit of themselves and their clients.

Wide Dynamic Range Cameras - The Best Feature for Video Cameras

By Steve McNeal |

The Wide Dynamic Range (WDR) feature on Security Cameras is one of the most important image improvements on cameras alongside the higher resolution cameras evolution we see in the security industry today. WDR is the camera's ability to see in contrasting levels of light such as when a camera is pointed towards a glass door or window, the background becomes "washed out" with the sun at different levels.

WDR is intended to provide clear images when the intensity of illumination varies in the FOV when there are very bright and very dark areas concurrently in the FOV. WDR corrects the image for the intense lighting surrounding an object and enhances the ability to distinguish features and shapes within the image.

Interesting enough, WDR is many times not the default setting on the cameras, and it should be. Every time I have started this feature on a customer's system, I always make sure the customer is present. When WDR is activated, the typical response is... , wow! The system response is details in all areas of the Field of View (FOV) and a brilliant picture. The customer first sees the benefit of the high resolution 1080p cameras, and believes that is a great picture, but once WDR is activated and they see the resulting image, the clarity and brilliance of the high resolution camera producing clear, low noise images with good contrast.

Normal WDR

Security video applications have various lighting situations that cannot be controlled; therefore the proper camera selection is critical to covering selected FOVs. In many video security situations there will be many locations with very contrasting brightness areas, which are not managed effectively by a standard non-WDR camera. Place a 1080p nice camera without WDR at the west-setting sun covering a parking lot, and you will get high-resolution flash-out with the results being useless video and poor results.

Camera with no WDR or WDR turned off Camera with WDR enabled

True WDR vs. Software WDR - Digital WDR (D-WDR) is a software-based technique that optimizes image quality by adjusting the gamma (γ) value to enhance dark areas. Digital WDR does not offer the same quality as True WDR. True WDR is achieved by a double exposure technique that takes one exposure with longer exposure time to get the detail in dark area. Then another exposure is taken with a shorter exposure time to get the detail in very bright areas. The two exposures are then combined into a single frame. WDR is a feature that would benefit most all camera locations and should be a requirement for any outdoor camera covering any critical areas.

Contact Security Video HD at 800-376-8408 or see us at http://www.SecurityVideoHD.com

Article Source: http://EzineArticles.com/?expert=Steve_McNeal