▶ EDITOR'S COMMENTS ... 1

▶PTZ Cameras 2

▶Monitor Employee Internet Usage ….. ... 3

▶Prevent theft corporate data……....4

Using Motion Detection…..5

Employee Security Awareness...6

Things to Stop on Facebook………..8

○ ISSUE 7 | ○ VOLUME 1 | ○ June 2010

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

As the use of CCTV proliferates some individuals develop a fixation on using Pan Tilt and Zoom (PTZ) cameras. There is the belief that because these cameras can be controlled by the user and pointed in different directions that they are a better option for persons who are about to install a new CCTV system. Our first article looks at **PTZ Cameras** and point out that they may not always be the right type for the particular security application.

In the modern business place, some employees would not be able to operate if they did not have Internet Access. A significant part of their job revolves around using the internet. For other employees the use of the Internet is not integral to the job but does ocassionaly play a role. Companies therefore often provide open access to the Internet. Our second article addresses why companies should **Monitor Employee Internet Usage**.

With the widespread use of computers in offices, access to corporate data has become easier and more widely distributed through organisations. Theft of corporate data however can often hurt a company more than a burglary or robbery. Our third article provides **5 Ways to prevent the theft of Corporate Data.**

Motion Detection is a useful feature found on most security DVR systems today. Our fourth article therefore addresses ways to **use Motion Detection for optimum benefit from your Cameras**.

While everyone accepts that employees operate in a security conscious manner, the organization benefits, the difficulty is to make **Employee Security Awareness** a fundamental aspect of operations. Our fifth article provides some pointers for achieving this.

Individuals are realizing that there are serious privacy and ultimately security issues when using Facebook. Our last article outlines some **things you should not do on Facebook**.

Is there anyone who you think would benefit from receiving this magazine? Just send their name and email address to newsletter@assl.com and we would be happy to add them to our mailing list.

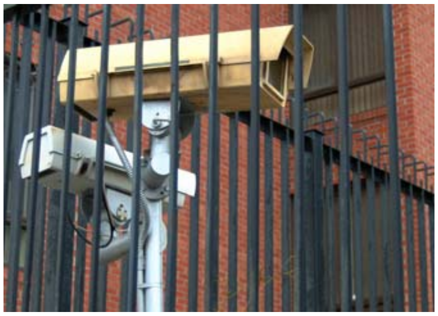
Brian Ramsey
Editor

PTZ Cameras

Learn the How, Where, When, Why and What to Avoid

By Alex Underwood

First off, lets define what a PTZ camera is. "PTZ" is an acronym used in the security and CCTV world for security cameras that can Pan/Tilt/Zoom using motorized or digital movements. These cameras can move their lenses horizontally (pan) and vertically (tilt), as well as change their focal length between near and far (zoom in or zoom out), and can be controlled from your DVR system or in some cases, even from your cell phone or computer over the internet.



Movable cameras while very useful in the right situation can also be useless and even harmful to the overall security of your property if used in the wrong situation or environment. PTZ's are most efficient when used to supplement an already well designed surveillance system. For example, if you rely solely on the PTZ for coverage you may be disappointed when your camera is facing the wrong direction when you need it most. However if you have designed a surveillance system around a number of fixed or Variable Focus cameras that give you excellent general view coverage, Guards, Security staff or the property owner can quickly and easily zoom in to get a closer look at what they have deemed an area that needs to be looked at more closely. Cameras can also be programmed to run a pattern or tour which allows for a general view of a wider area, though be prudent in their use, remember, you can only see the area where the camera is pointed.

Newer technologies allow for Pan Tilt Zoom cameras to auto-track objects or people of interest. This technology has its merit, though as of now, our experience is it is not quite reliable enough to use in a high security type of situation. Most Pan Tilt Zoom cameras use a 1/4" CCD chip, simply because the smaller chip size allows for smaller fields of viewing, a benefit in the case of a high powered zoomable CCTV camera. Most DVR systems or Digital Video recorders can control multiple PTZ cameras, though for advanced programming it is highly recommended to wire movable cameras so they can be controlled through the recorder or internet as well as through an external controller that can execute faster, and more advanced programming options.

PTZ camera uses vary widely but are a must for some such as Casinos and City Management for security coverage. Casino security must be able to close in on a cheater, thief, or out of control guest within seconds of noticing a problem in order to address the issue quickly and appropriately. Cities may use Pan/Tilt/Zoom cameras in order to watch traffic in one direction during morning commute and another during evening commute; they may also use them to zoom in on accidents or other incidents on the highway. For others, these cameras are a good fun way of keeping an eye on lazy contractors or simply making sure nothing is going on at your vacation property, and I must admit, they certainly are fun to play with.

PTZ cameras come in a wide variety of pan/tilt/zoom options such as; Degrees of movement, degrees of movement per second, as well a variety of focal lengths. Faster ones are called Speed-Domes and can operate at 300 degrees per second or more. The Zoom portion of the camera can come from two different methods of zooming. The preferred method is an optical zoom which actually incorporates a motorized lens with focusing and iris abilities, however, these models can run into the several thousands of dollars. For those looking to increase security with a panning, tilting or zoomable camera without busting the bank, check out cameras which feature a digital zoom. Much like your handheld photographic camera, these cameras can zoom in digitally with no moving parts. Images will become a bit pixilated, but the effect is the same.

When planning your CCTV camera system, consider what you've read when deciding if a movable camera is really what you need. In most cases, the cost of a single movable camera can be as much as three or four stationary cameras, so while it is a very cool and useful feature, it may or may not be right for your security application.

About the Author

Alex Underwood is Director of Product Development at CCTVDynamics. CCTV Dynamics is working to make high end security solutions available to every American who wishes to protect their property, their families and their businesses. We believe a secure home or business doesn’t need to break the bank. Find more about Alex and his recommended PTZ cameras at http://www.CCTVDynamics.com

Why Monitor Employee Internet Usage

By John W Sheridan

The monitoring of employee internet activity has been on the rise over the past decade. It is somewhat of a controversial subject with some employees saying it is unconstitutional. However, if done correctly and for the right reasons, one can argue that employers certainly have the right, legally and morally, to perform such monitoring.

Almost all companies that allow employees access to computers and the internet to perform their job responsibilities require the employee to sign a statement that outlines what is allowed by the employee as far as computer and internet usage.

In most cases it is clearly stated what are the penalties for not following these directives. In many cases it clearly states that the violation of these terms will be cause for dismissal. I truly do not understand why an employee, after signing such a statement, would have any reason to object to an employer monitoring his activity on his computer or internet.

There are many reasons that employers may decide to monitor employee internet usage.

Internet security is a major issue. Anytime one goes on the internet there is always a chance that your firewall or security program could be breached. We are talking about a computer being used that may have highly classified information about the company, its resources, and its employees. Any breach in security of your company's computers could be a major problem for the company and the employees as well.

File, program, and intranet security issues are involved. The employee decides to load up a program he brings in on disk or to show others working with him his latest vacation photos. The next thing you know he has caused a problem with the operation of your company's computer system. A file was over ridden, a file was deleted, a virus was on the disk he brought in and now the entire company's system is down. Information is lost.

Productivity of employees is certainly a concern. I think it is obvious that if an employee is using the internet for personal activities that this can decrease his productivity. It does not matter if it is visiting porn sites, gambling sites, sports office pools, doing their banking, shopping, or talking to their spouse or friend on an instant messenger, it will affect their productivity in a major way.

Just as a company has security guards in place to monitor traffic in and out of your company's work spaces you need to be sure that the same type of security is set up for internet traffic and activity. Years ago one only had to be concerned that the entrances and exits of your building were guarded. Well there is now an information highway that runs through your work environment that also needs to be kept secure.

There have been some exciting innovations in products that can assist an employer in keeping his computer systems secure, the internet usage by his employees under control and his employees productive!

5 Ways to prevent users from stealing corporate data

By Bill Detwiler

I'm Bill Detwiler, and during this episode of TR Dojo, I'll highlight five ways you can keep your data from walking out the door.

The first place to start with your users is to have a clear policy regarding the treatment of company data. Not everyone is a budding corporate spy, but a lot of damage can be done by careless or clueless users.

You may think it would be obvious to employees that they shouldn't copy important company information and take it home or email it outside the internal network without permission. But if you don't put such policies in writing and have workers sign for receipt, you may be hard pressed to penalize them for later violations.

Your policies should be specific and give examples of prohibited activities. Workers may not understand, unless you spell it out, that emailing a restricted company document as an attachment to someone outside the network (or even to their own home account) is just as much a violation of policy as copying that document to a USB drive and physically taking it out the door.

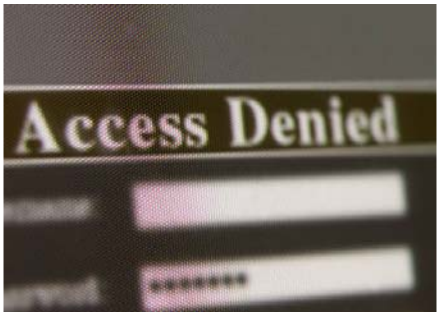
Wording of the policy, however, should make it clear that the prohibition is not limited solely to the examples you give.

The next step in protecting you data, once policies have been made clear, is technological enforcement of those policies.

Make sure you set the appropriate permissions on data files and folders. It goes without saying that data on Windows networks should normally be stored on NTFS-formatted drives so you can apply NTFS permissions along with any share permissions.

NTFS permissions are more granular than share permissions and apply to users accessing the data on the local machine as well as over the network.

In keeping with the principle of least privilege, you should give users the lowest level of permissions possible for them to get their work done. For example, give Read Only permissions to prevent users from modifying files.



You should also consider auditing files and folders that contain highly-sensitive data so that you can see who accessed it and when. You can do this with Windows Server's built in auditing tools or a third-party auditing solutions, such as:

- NTP Software File Auditor
- Blue Lance LT Auditor +
- isdecisions FileAudit

Another advantage of storing data on NTFS-formatted drives is the ability to apply Encrypting File System. And, using encryption is tip number three on our list.

EFS is supported by Windows 2000 and later operating systems and will prevent other users from being able to open the file even if they have NTFS permissions. With Windows XP/2003 and later, encrypted folders can be shared with other users by assigning them special permissions through the encryption dialog box.

And in the case of an entire computer being stolen, such as a laptop, Vista and Windows 7 Enterprise and Ultimate editions offer BitLocker full drive encryption to protect data in case of theft. And there are plenty of third-party encryption solutions, such as PGP Whole Disk Encryption and Check Point Full Disk Encryption.

The fourth way to prevent data from walking out the door is properly configuring of your firewall. Not only do firewalls keep undesirable traffic out of your network, they can also keep specified traffic from leaving your network. You can set up your firewall to block certain types of outbound protocols, such as those used by peer-to-peer software.

You can also set up your mail server to block sending of outbound attachments. And you can block outbound content by keywords using content filtering appliances, software, or services, such as:

1. Microsoft ForeFront
2. McAfee's MX Logic
3. GFI Mail Security
4. Google's Postini

Last, while taking care of the fundamentals, remember that your data can walk out your door in many different formats, some more creative than others.

A user can print out a document and carry it out in paper form or a thief can steal printed documents from trashcans if the documents haven't been shredded.

Even if you've implemented a technology such as rights management to prevent copying or printing documents, someone could take a digital or film photograph of the content onscreen or even sit and copy the information by hand. Be aware of all the ways your data can leave the premises, and you'll be one step ahead of the criminals who may be lurking in your midst.

During this episode, I've covered five ways to prevent employee data theft, but it's by no means an exhaustive list. Get more details and tips from Deb Shinder's article, "10 ways to make sure your data doesn't walk out the door," on which this video is based. I'll link to it in the TR Dojo blog.

And if you've come across an interesting or unique way that data can walk out the door, be sure to share it with us in the TR Dojo blog.

As always, for more teachings on your path to becoming an IT Ninja, visit trdojo.techrepublic.com, or you can follow me on Twitter at twitter.com/billdetwiler.

Reprinted from TR Dojo

Using Motion Detection to Optimize Your Security Camera System

By Alex Underwood

Motion Detection is a useful feature found on most security DVR systems today. Whether you're looking to optimize record times, count objects, utilize advanced search techniques, or trigger certain alarms, motion detection can be one of the most important features in turning your security system from a fancy gadget to a useful management and loss prevention tool.

Generally the DVR you purchase will be set up to record only when it detects motion in the video. Your system does this digitally when it notices differences in the pixels on the screen. Usually your system when it notices these differences will be triggered to start recording a few seconds before the motion, and a few seconds after, this is called pre-alarm and post-alarm recording. Pre alarm and post alarm recording not only saves a lot of hard drive space, it can also make searching for video much faster and easier by eliminating useless video data. DVR systems with Pre and post alarm triggers will also give you an entire event as they will retroactively save video that occurred before the system saw motion and will continue to record for a preset amount of time after the motion stops.

Most systems have sensitivity adjustments which will make more or less motion necessary before they start recording and it may take some tweaking to get your system setup properly. This applies to most PC based DVR systems as well as standalone DVR systems and the process can be a bit time consuming, but the benefits of going through the process far outweigh the setup time. After installing your security camera system, spend a few minutes each day looking over recorded video to find what motion events are causing the system to record. Then go through the motion masking features of your DVR system to mask out unwanted triggers. Remember, with pre-alarm and post-alarm recording, you can rest assured you will get the whole event whenever an object or person moves into the motion detection field, so don't be afraid to mask out unwanted motion triggers.

There are different levels of sophistication when it comes to motion detection - typically PC based DVR systems offer more features and enhanced sensitivity settings when compared to Standalone DVRs, but the principles are the same.

Most systems will include a grid overlay accessed in the setup menu for each camera. When we turn parts of this grid off we can tell the system to ignore motion in these areas, this is what we call motion masking. Much like masking tape helps a painter avoid painting trim pieces, the DVR uses the motion masking function to avoid triggering a recording condition in unwanted areas. This can be useful if our camera is detecting a tree blowing in the wind or a ceiling fan or even a monitor or Television. While PC based DVRs usually will have more detailed grids allowing more specific masking, a standalone DVR system may only have 9 squares that make up it's grid, so choose your DVR based on how precise you are going to want your masking and motion detection to be. Generally the more advanced your DVR system is, the more things we can do with motion detection, like trigger a siren or strobe light, some DVR systems will even send you an email or text message. Keep in mind, you will want your motion to be very accurate in order to use it as a trigger.

We can setup multiple motion detection zones which allow several benefits. We can count the amount of people that pass through a hallway or a point of sale area, count objects on a conveyor belt, or detect when an object passes through one zone but not another indicating theft. We can also setup motion detection zones where there shouldn't be any motion. When motion is detected the DVR system can sound an alarm notifying users of potential problems.

Regardless of what level of motion detection your system includes, you will find it a useful feature enhancing your surveillance system's usability and functionality.

About the Author

Alex Underwood is Director of Product Development at CCTVDynamics. CCTV Dynamics is working to make high end security solutions available to every American who wishes to protect their property, their families and their businesses. We believe a secure home or business doesn't need to break the bank. Find more about Alex and his recommended CCTV products at http://www.CCTVDynamics.com/articles.html

Employee Security Awareness

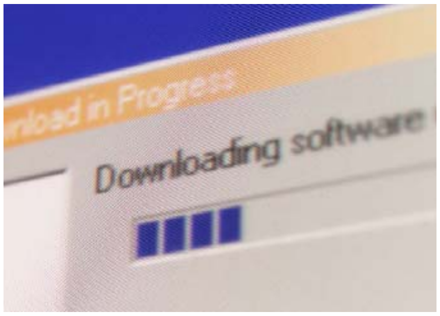
By Rick Spair

Playing Big Brother

No one wants to play the bad guy by monitoring every single action that a user makes. However, the unfortunate reality is that a good portion of security breaches are caused by staff members, whether inadvertently or intentionally.

Incidents of both kinds come in a variety of forms:

- Theft of credit card or other financial information by unethical employees.
- Opening infected e-mail attachments from unknown or untrusted senders.
- Forgetting to log off workstations at the end of the day.
- Disclosing passwords to coworkers, family, or friends.
- Installing unauthorized software on workstation PCs.



Act First, Think Later

It's one thing to foster a corporate culture that embraces security as a core value, but it's quite another to do so at the sacrifice of actual security technology investments. Gartner recommends that before companies even start thinking about implementing a security awareness program, they should:

- Solidify and strengthen all enterprise security systems and technologies.
- Establish formal practices and support for workers using these systems.
- Invest in security awareness only when the two previous steps are complete.

Action Plan

A successful security awareness program is one that compels all employees to take an equal share of the responsibility for the security of company assets. Bear in mind, however, that awareness alone can never replace comprehensive security policies.

1. Define your expectations for the users. Raising awareness ultimately means changing people's behavior. In addition to your existing non-disclosure and technology acceptable use policies, speak with HR to make employee information security responsibilities a condition of employment (strictly on a per case basis, of course). Also:
    - Give precise descriptions of what actually constitutes a security incident.
    - Establish concise instructions for reporting security breaches, events, or incidents.
    - Conduct basic security awareness "lunch and learn" sessions for staff members.
    - Be sure to clearly post all security-related documents on the company's intranet.
2. Make employees the centerpiece of attention. Stress partnerships and people, not technology and policing. Empower them by stating their critical role in information security. For example, avoid statements that say "Do this," or "Don't do that." Instead, use proactive, collaborative wording like "Your role is [...]," or "You can make a difference by [...]." Try to use disciplinary action as a last resort only
3. Measure the effectiveness of the program. Periodic security quizzes or tests are a good way to promote and measure the program's success among the employee base. Another method is to put a counter on the number of hits on the security documents section of the intranet. Where possible, employ power users within various departments to help you spread the word and make progress checks.

4. Communicate successes. Keep the lines of communication open with employees. Send out updates on existing and future security initiatives, as well as the background or rationale behind such decisions. If possible, set up a graphic security "barometer" on the corporate intranet to display the organization's current security status.

5. Keep the program flexible. What is considered a security best practice today might be obsolete tomorrow. Allow for some elasticity in your program, taking into account such factors as: changing business models and/or objectives; the introduction of new technologies; emerging security threats and/or new viruses; and growth of the network and the user base (i.e. resulting in a greater number of points of vulnerability).

6. Expect realistic results, not miracles. Malicious insiders in particular will remain difficult to stop by implementing a security awareness program, especially if they are determined to hack and burn. It's kind of like the federal government enacting a law that restricts the number of bullets allowed in a gun, and then expecting bank robbers to obey it. Still, simply conveying the repercussions of security breaches to employees will go a long way towards preventing them.

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

7 things to stop doing now on Facebook

Using a weak password
Avoid simple names or words you can find in a dictionary, even with numbers tacked on the end. Instead, mix upper- and lower-case letters, numbers, and symbols. A password should have at least eight characters. One good technique is to insert numbers or symbols in the middle of a word, such as this variant on the word "houses": hO27usEs!

Leaving your full birth date in your profile
It's an ideal target for identity thieves, who could use it to obtain more information about you and potentially gain access to your bank or credit card account. If you've already entered a birth date, go to your profile page and click on the Info tab, then on Edit Information. Under the Basic Information section, choose to show only the month and day or no birthday at all.

Overlooking useful privacy controls
For almost everything in your Facebook profile, you can limit access to only your friends, friends of friends, or yourself. Restrict access to photos, birth date, religious views, and family information, among other things. You can give only certain people or groups access to items such as photos, or block particular people from seeing them. Consider leaving out contact info, such as phone number and address, since you probably don't want anyone to have access to that information anyway.

Posting your child's name in a caption
Don't use a child's name in photo tags or captions. If someone else does, delete it by clicking on Remove Tag. If your child isn't on Facebook and someone includes his or her name in a caption, ask that person to remove the name.

Mentioning that you'll be away from home
That's like putting a "no one's home" sign on your door. Wait until you get home to tell everyone how awesome your vacation was and be vague about the date of any trip.

Letting search engines find you
To help prevent strangers from accessing your page, go to the Search section of Facebook's privacy controls and select Only Friends for Facebook search results. Be sure the box for public search results isn't checked.

Permitting youngsters to use Facebook unsupervised
Facebook limits its members to ages 13 and over, but children younger than that do use it. If you have a young child or teenager on Facebook, the best way to provide oversight is to become one of their online friends. Use your e-mail address as the contact for their account so that you receive their notifications and monitor their activities. "What they think is nothing can actually be pretty serious," says Charles Pavelites, a supervisory special agent at the Internet Crime Complaint Center. For example, a child who posts the comment "Mom will be home soon, I need to do the dishes" every day at the same time is revealing too much about the parents' regular comings and goings.

Reprinted from

June 2010 Consumer Reports Magazine.