International Council For Industrial Security & Safety Management

ICISS

Newsletter: August 2012

Let's professionalize the professionals…

http://www.wix.com/sbtyagi/iciss

ICISS

How safe are those full body scanners being used at airports?

Over the last few years, prisons and other security sensitive areas have begun using a device that scans the whole body for contraband. The scan produces an image of the skin, and will show objects like guns, drugs, other weapons under clothing. This procedure is often used an alternative to whole body strip searches. The device uses a low energy x-ray or gamma source to produce the image.

The draw backs to this are 1) privacy issues; 2) radiation dose to the individual; 3) radiation dose to the workers. The next time you go through security at the airport, you might be told to empty your pockets, put your hands over your head and stand still while an X-ray machine looks for anything hidden under your clothing.

If this body scanning option sounds unappealing, you have another choice: an "enhanced pat down" conducted by a Transportation Security Administration employee, which some travelers have described as quite intimate.

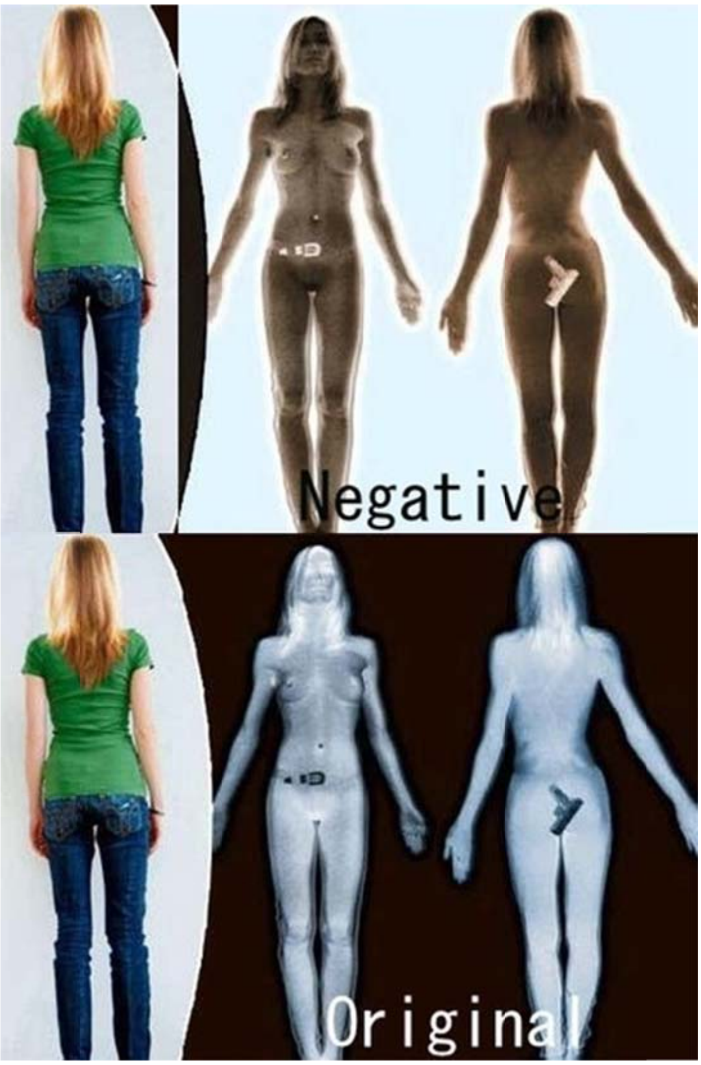
The new screening measures have been hotly debated, but mostly in theory. Now that in USA there are nearly 244 body scanning machines in about 50 domestic airports, with 800 more on the way, passengers are facing real-life decisions about what to do. Here's some information to help you choose.

How Do the Machines Work?

If you somehow missed the hoopla, there are two types of machines being installed, which

have raised concerns about privacy, health risks and even their effectiveness at catching terrorists. The more controversial “backscatter” devices project an X-ray beam onto the body, creating an image displayed on a monitor viewed in another room. The “millimeter wave” machines, which are considered less risky because they do not use X-rays, bounce electromagnetic waves off the body to produce a similar image.

Unlike metal detectors, these machines can detect objects made with other materials, like plastic and ceramic. But they can’t see anything hidden inside your body, or detect certain explosives.



What Can Screeners See?

What these images reveal is also unclear. Mr. Kimball said that the T.S.A. uses filters to blur the images, and the agency has posted samples of the kinds of images screeners see and a video of the screening process on its Web site, tsa.gov. But critics say these samples aren’t detailed enough for travelers to judge how explicit they are, especially if a screener zooms in on a specific area.

Another concern is whether the images can be saved or transmitted. The T.S.A. first said this wasn’t possible, then later admitted the machines can save photos, but that this feature had been disabled. This kind of backtracking has added to the agency’s credibility problem.

How Safe Are They?

The main concerns are how much radiation the scanners give off (the manufacturers say the amount is very low), whether the scanners might malfunction and emit more radiation than they are supposed to, and what the health effects may be for travelers. Since there is no precedent for routinely screening so many people with X-rays - other than in prisons - there are a lot of unknowns.

Another issue is that the devices haven’t been thoroughly tested. The T.S.A. (Transportation Security Administration, USA) claims that the machines have been evaluated by the Food and Drug Administration’s Center for Devices and Radiological Health, the Commerce Department’s National Institute for Standards and Technology and the Johns Hopkins University Applied Physics Laboratory. But it is confirmed that they basically tested only one thing - whether the amount of radiation emitted meets guidelines established by the American

National Standards Institute, a membership organization of companies and government agencies.

But guess who was on the committee that developed the guidelines for the X-ray scanners? The representatives from the companies that make the machines and the Department of Homeland Security, among others. In other words, the machines passed a test developed, in part, by the companies that manufacture them and the government agency that wants to use them.

‘Russia Today’ points out an important detail being left out of most mainstream media reports about the new body scanning devices being rolled out in airports everywhere: former Department of Homeland Security Chief, Michael Chertoff, who has been advocating this technology on any news program that will have him is personally profiting from their implementation. As a Security Consultant and Chairman of the Chertoff Group, one of his main clients is Rapiscan, a manufacturer of these devices.

Last year, the Department of Homeland Security awarded contracts of US$160 million each to two manufacturers of these back-scattering devices, one which was Rapiscan.

Beyond the issue of Chertoff's illegal advertising his product on news programs by pretending to be a public servant, there is some debate about the safety of these new Back-scatter X-Ray Body Scanning devices.

One former intelligence agent and present-day security consultant, Wayne Simmons, says that while the device is an excellent tool, "There is no dose of backscatter ionizing radiation that has ever been proven safe," and that he would prefer to see only passengers who are deemed to be suspicious going through these devices, with the bulk going through the metal detectors, with which we've all become accustomed.

In lighter veins

John Wayne's Five Rules

1. Money can't buy happiness but it’s more comfortable to cry in a Mercedes than on a bicycle.

2. Forgive your enemy but remember the bastard's name.

3. Help someone when they are in trouble and they will remember you when they're in trouble again.

4. Many people are alive only because it’s illegal to shoot them.

5. Alcohol does not solve any problems, but then again, neither does milk.

Transitioning Alarm Monitoring from In-House to a Third Party!

By Capt G Raj Kumar

The alarm monitoring and response is very complex and tedious function of Security Management. Fraught with False Alarms and resource-mobilization, alarm monitoring also means that systems need to be constantly upgraded and procedures checked. There is also need to constantly audit the efficacy of the system, return-on-investment and the integrity of the data for very efficient alarm monitoring. Since all these activities occupy lot attention and priorities of the organizations, the forward looking managements started off-loading these activities to third-parties – specialist in the field. This turns out to be cost effective and very dependable option which enhances the level of security preparedness.

Capt G Raj Kumar is ICISS Councilor for Andhra Pradesh.

He has total 25 years of experience out of which he served 14 years in the Armed Forces and rest 11 years in the industry. He has unique distinction of serving in Air forces as well as in Army. While in Armed Forces he has been extensively involved in Counter Insurgency Operations.

He holds degree of MBA (HRD) from Rani Durgavati University, Jabalpur. Presently he is pursuing a Ph. D in Personnel Management. At present he is working in GAIL and posted at Vizag, Andhra Pradesh.

A keen sports enthusiast, he represents Andhra Pradesh Badminton Team. Previously he has played in badminton tournaments conducted by Petroleum Sports Control Board of India.

He can be reached at grajkumar@gail.co.in or on his Mobile number - 7893601699.

Spearheading this phenomenon are few security agencies who have established their Central Monitoring Stations in cities all over. These centers cater to big offices, industries as well as individual residents who wish to avail their services. Large industries are in process of getting third party monitoring services and the process seeks our well laid-out strategies.

A monitoring center must provide timely, consistent, high-quality services utilizing state-of-the-art technology to customers 24 hours a day, 365 days a year. Keeping pace with the changes in technology and maintaining alarm system data integrity were crucial to maintaining goal of providing best-in-class alarm monitoring service. In addition to equipment needed, enhancing alarm data integrity is also necessary to ensure the highest level of security is continuously maintained. The planning phase may include five critical elements which would become foundation to successfully convert in-house alarm monitoring platform to a third-party supplier:

- Transition team identification
- Decision process to determine the service provider
- Project planning
- Implementation

- Post implementation (continuous improvement)

Transition Team

To successfully convert alarm monitoring to a third-party supplier, a transition team of customer-focused leaders may be selected to design, analyze, and implement the alarm monitoring transition project. In addition to loss prevention, transition team is to include stakeholders from the following departments: procurement, finance, business unit leaders, IT, real estate, legal, facilities, and operations etc. This team must meet regularly, defining the objectives, building success criteria, creating performance metrics, and representing the organization to ensure a seamless transition of alarm monitoring.

Any plan for the alarm monitoring transition may include:

- Understand the buy – interview stakeholders
- Establish operating procedures for supplier
- Develop draft scope of work for review by stakeholders
- Present sourcing strategy (scope of work, list of suppliers, and timeline)
- Develop, distribute, and analyze request for information
- Complete supplier bid meetings and site visits
- Suppliers complete and return request for information
- Present request for proposal (RFP) supplier short list recommendations to stakeholders
- Analyze RFP
- Negotiate with suppliers
- Present overview to stakeholders
- Notify suppliers and stakeholders of contract award
- Execute contract
- Develop performance metrics
- Establish quarterly performance meetings to review and track performance metrics

Determining the Service Provider

Collectively, transition team needs to identify suppliers that provided the most comprehensive, customer-focused capabilities. Criteria for a successful service provider are as following:

- Fitness to technical and functional requirements
- Total cost of ownership
- The ability to support current and emerging equipment
- Industry reputation and experience
- Experience and qualifications of the company and resources
- Quality assurance commitment
- Financial strength
- Proven methodologies, tools, and value added services

Sourcing decision must be based on the “best value/total cost” principle. While cost remains a critical decision factor, the quality of the equipment, and operating efficiencies would be the primary and most critical aspects.

Project Planning

A project task list can be created to identify key issues that can affect the overall project and allow assignment of tasks. Tasks can be assigned milestones in the project file to help balance workload for project planning. Clear communication, precise operating procedures, and partnership with selected solutions provider are the building blocks of our transition plan.

Implementation

Converting alarm system monitoring, whether from in-house to third party or third party to in-house, requires absolute understanding of a defined scope of work. To implement the alarm system monitoring change, the data from the existing monitoring facility can be gathered and scrubbed to determine its accuracy and freshness. The data then need to be formatted in order to be inserted into new monitoring systems and reviewed again for accuracy. Once all data is in place in new monitoring systems, the stage is set to develop the schedule for the change-over.

Post Implementation – Continuous Improvement

The alarm monitoring conversion from proprietary monitoring platform to the Third party Monitoring Center has to be a seamless, successful event. Metrics need to be assigned to all the alarms and responses. Each metric was assigned a target goal, for example 90 percent of burglar alarms within 60 seconds. To ensure continuous improvement, it is advisable to develop quarterly performance business reviews. Business reviews provide the avenue to assess performance metrics, identify opportunities to strengthen partnership, and continue to focus on achieving both organizations' internal and external goals.

A monitoring center must provide timely, consistent, high-quality services utilizing state-of-the-art technology to customers 24 hours a day, 365 days a year. Keeping pace with the changes in technology and maintaining alarm system data integrity were crucial to maintaining goal of providing best-in-class alarm monitoring service.

In addition to equipment needed, enhancing alarm data integrity is also necessary to ensure the highest level of security is continuously maintained. The planning phase may include five critical elements which would become foundation to successfully convert in-house alarm monitoring platform to a third-party supplier:

- Transition team identification
- Decision process to determine the service provider
- Project planning
- Implementation
- Post implementation (continuous improvement)

Transition Team

To successfully convert alarm monitoring to a third-party supplier, a transition team of customer-focused leaders may be selected to design, analyze, and implement the alarm monitoring transition project. In addition to loss prevention, transition team is to include stakeholders from the following departments: procurement, finance, business unit leaders, IT, real estate, legal, facilities, and operations etc. This team must meet regularly, defining the objectives, building success criteria, creating performance metrics, and representing the organization to ensure a seamless transition of alarm monitoring.

Any plan for the alarm monitoring transition may include:

- Understand the buy – interview stakeholders
- Establish operating procedures for supplier
- Develop draft scope of work for review by stakeholders
- Present sourcing strategy (scope of work, list of suppliers, and timeline)
- Develop, distribute, and analyze request for information
- Complete supplier bid meetings and site visits
- Suppliers complete and return request for information
- Present request for proposal (RFP) supplier short list recommendations to stakeholders
- Analyze RFP
- Negotiate with suppliers
- Present overview to stakeholders
- Notify suppliers and stakeholders of contract award
- Execute contract
- Develop performance metrics
- Establish quarterly performance meetings to review and track performance metrics

Determining the Service Provider

Collectively, transition team needs to identify suppliers that provided the most comprehensive, customer-focused capabilities. Criteria for a successful service provider are as following:

- Fitness to technical and functional requirements
- Total cost of ownership
- The ability to support current and emerging equipment
- Industry reputation and experience
- Experience and qualifications of the company and resources
- Quality assurance commitment
- Financial strength
- Proven methodologies, tools, and value added services

Sourcing decision must be based on the “best value/total cost” principle. While cost remains a critical decision factor, the quality of the equipment, and operating efficiencies would be the primary and most critical aspects.

Project Planning

A project task list can be created to identify key issues that can affect the overall project and allow assignment of tasks. Tasks can be assigned milestones in the project file to help balance workload for project planning. Clear communication, precise operating procedures, and partnership with selected solutions provider are the building blocks of our transition plan.

Implementation

Converting alarm system monitoring, whether from in-house to third party or third party to in-house, requires absolute understanding of a defined scope of work. To implement the alarm system monitoring change, the data from the existing monitoring facility can be gathered and scrubbed to determine its accuracy and freshness. The data then need to be formatted in order to be inserted into new monitoring systems and reviewed again for accuracy. Once all data is in place in new monitoring systems, the stage is set to develop the schedule for the change-over.

Post Implementation – Continuous Improvement

The alarm monitoring conversion from proprietary monitoring platform to the Third party Monitoring Center has to be a seamless, successful event. Metrics need to be assigned to all the alarms and responses. Each metric was assigned a target goal, for example 90 percent of burglar alarms within 60 seconds.

To ensure continuous improvement, it is advisable to develop quarterly performance business reviews. Business reviews provide the avenue to assess performance metrics, identify opportunities to strengthen partnership, and continue to focus on achieving both organizations' internal and external goals.

CCTV: Fundamental flaws and potential improvements

CCTV systems have one fundamental flaw – despite putting up large numbers of cameras to maximize the coverage of an area, we seldom have anybody actually looking at much of the area for which we are responsible.

Sure, we can always go back and look at what happened, but many times this just is not good enough. It is a problem of logistics and economics. We cannot staff the control room with enough people to view the number of cameras we have available. So we have many of these cameras' views going to waste when it may be useful to view them.

To make it worse, much of what is displayed on monitors will be uneventful, or sometimes even have content that is irrelevant to the risk profile of the site. This problem of coverage is not likely to go away soon. However, there are technologies being implemented now or in the near future that will change the risk coverage by CCTV significantly.

Intelligent technology that is being developed can help in a number of ways. Central to this is technology that can work with the operator in the background performing intelligent analysis of the camera views.

- Firstly, the computer can do things that computers are good at, and free the operator up to concentrate on other duties. For example, where automated recognition such as face recognition or number plate recognition can do the job, it frees the operator up to concentrate on the more relevant things that only people can do. In this way it is optimizing the use of the system.

- Secondly, background sensing and alerts or alarms allow the detection of suspect conditions on cameras that are not currently being viewed by the operator. The computer can highlight these or bring these to the operators' attention for viewing and investigation. This could include certain types of movement or the presence of somebody or something in an area for defined periods. Through this, the coverage of the cameras has been made more efficient.

- Another option is acting as an early warning system. In this context, the technology can highlight conditions that could potentially be suspect such as objects left in an area; cars parked where they should not be, or excessive densities of people in an area. This technology is starting to become more common with advanced DVR systems.

Potential Areas of Developments:

Other technologies offer substantial potential, but have some development time still to go before they reach effective use. Where an operator is viewing a scene and needs to divert his or her attention to something else, parallel monitoring or tracking through tagging a particular object or person could allow operators to come back to that scene later and pick up more easily on the location and movement of the target. Building up an information base on targets, situations, and behaviors to use for risk management and future investigation is one of the most neglected aspects of CCTV.

Intelligent Technology:

Use of an intelligent system that recognizes behavior and conditions can greatly help by increasing the amount and quality of information coming in. Technology can also help by simulating or verifying operator performance, either in contrasting the number of issues picked up by the intelligent systems, or the insertion of scenarios that should be picked up by operators and reviewing them against actual detection scores. Finally, intelligent technology can be used to extend the normal CCTV functions by building in algorithms that allow the detection of other things such as fire, smoke, production stoppages, overflows and so on that would add value to the CCTV function. I think the potential for intelligent analysis, sometimes called visual analytics technology, goes far beyond security-based CCTV to many forms of risk management and monitoring. The questions on “what, where, when, who, why and how” will increasingly become available in our data retrieval system.

Implementation Problems:

Besides the development needs that are required to realize some of the ideas for technology, there are some implementation problems with those we already have available. Cry wolf is when repeated warnings occur without foundation. Eventually, the people start disregarding the warnings and the potential of the technology becomes ignored.

Use of blank screen-based alarm systems are a classic example, after 90 false alarms popping up on screen in an hour or two, the screens often get switched off because they are just seen as a distraction. We can also overload the operator with warnings on what could be happening so that they do not have the time to deal with everything they are faced with. Priority setting in such instances becomes important. We do not want CCTV to be reactive to only technology-based detection - people are still more efficient at being proactive and picking up dynamics and behavior. If we prevent them searching for incidents, we will probably miss some of the most important. The timing of the event occurrence, or when we warn the operator is also something that needs to be considered. Too soon may just provide a lot of false alarms, too late may be exactly that - too late. Finally, where do we place the warnings within the display environment - does it become the center of attention, or one of the tools the operator uses.

Envisaged Improvement in performance: Technology has the potential to deliver higher performance in a number of ways:

- ***The level of work being performed* -** people can concentrate on the important and higher priority issues that need human interpretation.
- ***The volume of coverage of the system* -** all of these cameras are really working - not just providing a mass of information that will largely be lost and discarded. Clients are getting real capital return on their system investment. Event generated alarms and video monitoring and tracking helps! Privacy ensuring blockage of pre-determined areas help greatly in avoiding litigations on breach-of-privacy related matters.
- ***The quality of results delivered:*** This is surely going to provide higher security related out-put: more things are being detected, and the base is being laid for a more intelligence and directed risk management process.

In five years' time, we will find intelligent systems on just about every worthwhile CCTV site. However, despite all the limitations with CCTV systems, the operator is still the key and final decision maker. The right operators make a significant difference to the system. Operators will continue to be able to do things that technology is unable to do and will do so for some years to come.

Thieves and Criminals outside your door steps?

Courtesy: Col Deepak Behl

Pretty neat idea! Never thought of it before!!
Put your car keys beside your bed at night

Tell your spouse, your children, your neighbors, your parents, your Doctor's office, and the check-out girl at the market, everyone you run across. Tell them to 'Put your car keys beside your bed at night'. If you hear a noise outside your home or someone trying to get in your house, just press the panic button for your car. The alarm will be set off, and the horn will continue to sound until either you turn it off or the car battery dies. This tip came from a neighborhood watch coordinator. Next time you come home for the night and you start to put your keys away, think of this: It's a security alarm system that you probably already have and requires no installation.

Test it.

It will go off from most everywhere inside your house and will keep honking until your battery runs down or until you reset it with the button on the key fob chain. It works if you park in your driveway or garage. If your car alarm goes off when someone is trying to break into your house, odds are the burglar/rapist won't stick around. After a few seconds all the neighbors will be looking out their windows to see who is out there and sure enough the criminal won't want that. And remember to carry your keys while walking to your car in a parking lot. The alarm can work the same way there. This is something that should really be shared with everyone. Maybe it could save a life or a sexual abuse crime.

Food for thought:

If it is not already with you, provably it will harm you: the information, the technology – in short, 'The Edge'!

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!

Suggestions & feedback may be sent to us on e-mail: sbtyagi1958@gmail.com