International Council For Industrial Security & Safety Management

Newsletter: October 2012

Let's professionalize the professionals…

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

More and more resources of the Governments world over are committed to combating the trans-border crimes, international terrorism and geo-political disagreements. There is tremendous pressure on the governments to resolve the social, cultural and financial disparities and disputes. The societies are in upheaval and the churning has started for radical change in the whole approach governments have taken to administer and govern.

The industrialization has brought in new dimension of crimes – industrial crimes and also focused the attention very sharply on the needs of "Industrial Security". The global aspirations of the countries especially the developing ones can only be realized if global benchmarks are to be achieved.

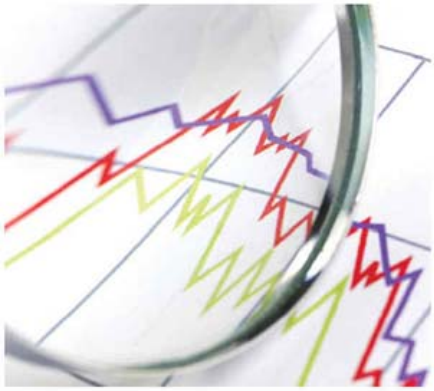
The industries therefore need uninterrupted operation and congenial industrial relations with the employees, customers and general public at large. The industry specific security need can be met by only the specialized security force.

In the complex situation in which security concern of the industries need to be answered and governments' resources found to be limited, the silver-lining appears indicating that there is possibility of 'Public and Private Partnership' (PPP) which will strengthen the governments' limited resources and qualitatively improve the security measures for the industry.

Capt S B Tyagi
For ICISS

Top Seven Physical Security Trends

The overarching change in physical security is a shift from analog to IP systems and networks. This movement has major implications for equipment purchases, processes, staffing, and training. In the article are seven of the most significant trends in IP-based physical security and how they help you prepare for, protect, detect, assess, and respond to threats.



IP Devices Replace Analog at an accelerating Pace

Organizations will continue implementing more IP-based video surveillance cameras, building access controls, and sensors over analog devices. The main reason is that IP networks provide capabilities not available on proprietary networks, such as:

Quality of Service (QoS)

You can assign priority to data based on the application type, sender, or recipient. Surveillance video, for example, needs priority over other types of application traffic sharing the same network. Furthermore, during disaster response, you can assign priority to all critical information to and from commanders and executives, making sure that these messages don't have to compete with less urgent communications.

Discovery protocols

The network automatically discovers new nodes, such as sensors, cameras, or wireless access points, eliminating the time and effort of manual provisioning. IP-based discovery protocols are especially valuable today, when IT departments are stretched thin.

Authentication and authorization

An especially popular technology is Network Admission Control (NAC), which authenticates both the user and the device before granting network access. If the device doesn't comply with the organization's security policy, NAC can remediate the device automatically, with no involvement by the IT organization.

To be sure, analog security devices won't disappear anytime soon--especially given today's limited budgets for new purchases and the time required for re-training. However, organizations are discovering that they can increase the value of their existing analog cameras and sensors simply by connecting them to the IP network.

Surveillance Video Becomes Life-Like

New high-definition (HD) video surveillance cameras provide resolution of up to 1080p and 30 frames per second, vastly increasing the value of video surveillance. With HD video, organizations can:

- Identify people with confidence. A clear video clip creates powerful evidence for prosecution or exoneration.
- Read license plates at distance.
- Use video analytics software (see next section).
- And generally do a better job of identification and assessment.

However, more pixels take up more bandwidth. So unless HD video surveillance cameras are paired with effective compression algorithms like H.264, some organizations may require additional bandwidth. We expect to see the gap narrow through 2009.

Video Analytics Software Continues To Mature

Video analytics software can be hosted centrally on dedicated servers or in individual cameras. It offloads human operators by tirelessly counting people, identifying unattended packages, recognizing license plates, detecting motion, and more. After identifying an event of interest, the software can automatically alert a human operator, and perhaps send the video clip along with the a

Trends in video analytics include

- Greater reliability and stability, resulting in more actionable information.
- Decreasing prices, making it practical for new types of applications, such as loss prevention in retail environments.
- Processing in the video surveillance camera itself rather than on centralized servers. Cisco IP Video Surveillance Cameras, for example, have the onboard intelligence to identify events of interest, eliminating the need for more bandwidth to accommodate high-definition video sent constantly from multiple cameras.

- Applications in addition to physical security. Retailers, for example, have begun using video analytics to recognize when lines get too long. An alert is sent to the manager, who can adjust staffing.

Building Controls Go IP

Organizations are beginning to shift their building access controls from isolated networks to the same IP network they already use for voice, surveillance video, and data. Harrisonville Schools in Missouri uses an IP-based building control system to automatically enforce policies stating when doors should be locked or unlocked. Administrators no longer worry or have to go around and check individual doors, and they like knowing that they can quickly lock down the entire building with a single click.

We'll continue to see more organizations integrate their IP-based video surveillance and building control systems, to improve incident detection and assessment. An attempt to use an access card, for example, can trigger the video surveillance camera to capture the event, and either send an alarm or archive the video for forensics purposes. We are also seeing organizations integrate the network-enabled building systems and device power management--for example, to turn employees' IP phones on or off when they swipe an access badge.

Open Standards Come of Age

In today's economic climate, organizations are keenly aware that their investments will likely have to last a long time. Solutions built with open standards are easier to expand, customize, and integrate with other solutions.

Organizations like Open Network Video Interface Forum (ONVIF), Physical Security Industry Association (PSIA) and the Security Industry Association (SIA) are leading the adoption of open standards. Examples include H.264 for video compression and Common Alerting Protocols (CAP) for broadcasting alerts to up to tens of thousands people at the same time, whether they are using a mobile phone, smartphone, telephone, IP phone, or laptop. Not surprisingly, security system resellers and integrators are flocking to sign up training to learn or refresh their IP skills. Many consider fluency with IP a requirement for business survival.

Radio Interoperability Grows Into Communications Interoperability

It will take years, if not a decade or more, before every public- and private-sector organization can find the budget to replace its radios. What's more, it's become clear that collaboration within and between organizations requires more than radio interoperability. People who are out

of radio range need to be able to join talk groups with traditional phones, IP phones, mobile phones, or laptops. And they also want to share video, floor plans, database access, and each other's desktops. The trend is towards comprehensive communications interoperability, and it has taken hold in public and private sectors:

- The City of Danville, Virginia, uses the Cisco IP Interoperability and Collaboration System (IPICS) to enable communications interoperability among multiple agencies along the Virginia and North Carolina border.
- Auckland International Airport in New Zealand uses the same solution to enable operations center personnel to monitor any radio channel from a PC any desk instead of finding a desk that has the appropriate physical radio.
- Bryant University, of Rhode Island, hosts an IP-based interoperability and collaboration that it shares with multiple local and state agencies, helping to create a safer environment not only on campus, but in the larger community.

The Demise of Standalone Systems

Customers today are far more likely to ask for complete solutions. Lean IT departments are growing leaner, and IT personnel simply don't have the time or budget to integrate proprietary point products. Nor do security personnel have the staff to use separate management interfaces. Out-of-the-box integration based on common open standards is the key. Recognizing this, vendors are establishing partnerships to ensure that their solutions interoperate. As an example, the Cisco Open Platform for Safety and Security provides a framework for systems integrators to use commercial, off-the-shelf (COTS) products. Use of COTS products reduces costs and enables organizations to integrate more capabilities from different vendors as their needs change.

Conclusion: A Simple Plan to Harness the Advances

Collectively, these trends help organizations improve their ability to prepare for, prevent, detect, assess, and respond to threats. Organizations can take advantage of the advances in the following phases, as budget permits:

- Connect existing video surveillance cameras and sensors to the IP network so that you can securely monitor them from any location, using a Web browser.
- Add IP-based building access controls and communications systems.
- Implement policy-based response to detected events--for example, notifying a security guard on a smartphone if a door is opened after hours or a sensor reading is out of normal range.



Women's Safety in India

By: Col Sushil Pradhan, MitKat Advisory Services

Violence against women is becoming a trend in India. In August 2012, Pallavi Purkayastha was attacked and killed by a watchman in her bedroom in her Mumbai apartment. Over the last few years there have been highly publicized cases of misbehavior, rape and even murder of BPO employees by cab drivers/assailants, followed by an outrage in the media for few days.

Earlier this year, in Guwahati, a teenager was groped, violated, molested for more than 30 minutes in full public glare; the subsequent insensitive handling of the incident by political leaders and constitutional authorities left a lot to be desired. In other key economic centers of India like Pune, Bangalore, Gurgaon, Noida etc. the cases of eve teasing and molestation are on the rise. Unfortunately, the law remains ineffective. Molestation is a cognizable, but bailable offence in India.

An ASSOCHAM survey in 2008 had highlighted that 86% women on night shifts face commuting problems; most felt their employers were not taking enough steps to ensure their safety. The situation may have improved but only slightly. In contemporary India, where there have been incidents of abduction, rape and murder, women have to take extra precautions to stay out of vulnerable situations that could lead to physical or emotional harm.

Crimes against women are not unique to India. This is how the British journalist Natasha Smith narrated her ordeal in Tahrir Square, Cairo on 24th June 2012:

"Men began to rip off my clothes. I was stripped naked. Their insatiable appetite to hurt me heightened. These men, hundreds of them, had turned from humans to animals. Hundreds of men pulled my limbs apart and threw me around. They were scratching and clenching my breasts and forcing their fingers inside me in every possible way. All I could see was leering faces, more and more faces sneering and jeering as I was tossed around like fresh meat among starving lions."

About the author

Col Sushil Pradhan is an army veteran with extensive experience in India and abroad on defense strategies and also on industrial security management.

With numerous published articles to his credit, he is presently Director Geo-Political Risk Management with MitKat Advisory Services.

He can be contacted at sushil.pradhan@mitk

Few days later, still recovering from the trauma, she said, "I knew there are huge risks as a woman, when travelling to different parts of the world. But, I did not quite realize how rapidly a situation could transform from a peaceful celebration involving women and children, to a vicious attack, led by male mob mentality. I'll never know for certain why those men did what they did. I do know that mob mentality is an extremely powerful thing. My heart goes out to all women, who are forced to continue to venture outside alone, after suffering these kinds of

sexual assaults, as it's a painful and terrifying ordeal. But, this is a struggle that unifies women across borders who are suffering regular and systematic abuse and assault..."

Legal Aspects

The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Bill, 2010, was recently passed in the Lok Sabha on September 3. Some of the important provisions of the bill are:

- The bill makes it mandatory for an employing company to set up a 'local complaints committee' which is headed by a woman. These will look into complaints of harassment. The employer will be held responsible for any lapse.
- The bill covers all women in workplaces including schools, colleges, hospitals and domestic help.
- Women can complain against any unwelcome direct or indirect sexual implication, sexual advances or requests.
- Women who have been sexually harassed will be entitled to compensation.

Though the bill is seen as much-delayed pro-women legislation, there have been concerns as well. Amongst others, there is an option for conciliation of the issue on the request of the complainant woman, which may lead to abuse of the law. It also leaves out women employed in agriculture, construction and in the Armed Forces.

What Should Women Do?

- Trust your instincts about people and situations; be alert and aware about your surroundings. If you sense danger or feel someone is following you, step into a crowded place (but not too crowded). Call a friend or relative to escort you back.
- When getting into or out of your car, watch out for anyone hanging around or a single man in any car parked near yours. Run back to safety if you are suspicious.
- Walk confidently. Do not appear nervous or afraid. Criminals tend to target scared-looking, nervous women.
- If the assailant has a gun, run away as fast as possible; there is a fair chance that he will not shoot; and even if he does there is an even greater chance that the bullet would miss you.
- Keep Police Control room numbers or another emergency number of a friend or relative on your speed dial.
- You could keep a pepper spray handy; if not, at least have a perfume or hair spray.
- Learn self-defense techniques; the law permits self-defense, including use of force.

- Be polite, but careful. Never open the door to a stranger when alone nor stop to help a man in deserted area; you can call the cops or inform office 24x7 control room if you want.
- When a mechanic or plumber or electrician is due for work at home, please ask your husband, neighbor or friend to be present.
- Do not leave door keys in obvious places (like near the main door).
- Dress appropriately and avoid flashing wealth; do not invite trouble.
- Keep away from mobs. "In a mob, every individual has the potential to turn into a violent criminal." Victimizing a woman comes easy in patriarchal societies.

Technology to the Rescue - Mobile Apps for Women Safety

With mobile phones having become such inseparable part of our lives, women can definitely make good use of technology to use their mobile phones as an SOS tool in case of emergencies. There are some easily downloadable apps available that can help enhance the safety and security of women, everywhere and every time.

- FightBack makes use of GPS, SMS, location maps, GPRS, e-mail and your Facebook account to send SOS alerts to a pre-defined list of emergency mobile numbers in case of any emergency.
- EyeWatch has some additional features. Free fall activation means the application gets activated by itself when mobile phone drops (dropping a mobile is a common occurrence in emergency situations). The inbuilt audio/video/image support enables the application to even send the images, videos and sound bites along with the location in SOS alerts.
- 'I Am Safe' can notify well-wishers and the nearest police station just by the press of a button in case of emergencies. The app also lets your family members or friends track if you're travelling in a cab in the right direction.

- Life360 Family Locator enables you to track the location of the person via GPS technology. You can also get details of safety points like hospitals, police and fire stations in your neighborhood.
- One Touch Location enables a woman leaving from office at night to send her current location at one click to family and friends, who will also be able to track the current location as she travels back.

There are likely to more such apps available in the online market-place. However, what's important is to get one, get used to it and use it in case of an emergency. If you are a working woman, let people at your work-place know that you have such an app on your phone. Such awareness by itself can be a deterrent to at least those in the know. Use technology to your advantage and stay safe, ladies.

Note: This article has reference to MitKat Women's Safety Guide 2012, an article titled "Women Stay Safe!" published in Times Life on 26 Aug 201, a blog by Natasha Smith and a feature that appeared on rediff.com

New lab working on security shoe sole to ID people

Nike-Shoes.Jabong.com

A new lab is working to perfect special shoe insoles that can help monitor access to high-security areas, like nuclear power plants or special military bases.

The concept is based on research that shows each person has unique feet, and ways of walking. Sensors in the bio- soles check the pressure of feet, monitor gait, and use a icrocomputer to compare the patterns to a master file for that person. If the patterns match the bio-soles go to sleep. If they do not, a wireless alarm message can go out.

"It is part of a shoe that you do not have to think about," said Marios Savvides, Head of arnegie Mellon University's new Pedo- Biometrics Lab, in Pittsburqh. The lab, which has $1.5 million in startup funding, is a partnership with Autono- mous ID, a Canadian company that is relocating to several U.S. cities. Todd Gray, the company President, said he saw the potential when his daughter was in a maternity ward decorated with representations of different baby feet all along a wall.

Autonomous ID has been working on prototypes since 2009, with the goal of making a relatively low cost ID system. Gray said they have already run tests on sample bio-soles, which are no thicker than a common foot pad sold in pharmacies, and achieved an accuracy rate of more than 99 percent. He said Carnegie Mellon will broaden the tests to include "a full spectrum of society: big, tall, thin, heavy, athletic, and multicultural, on a diet, twins and so on." Gray would not speculate on what the system will cost or when it might reach the marketplace, but each worker at a site would have his or her own pair of bio-soles. "Within the third step, it knows it is you, and it goes back to sleep," he said. "If I put on yours, it would know almost instantly that I am not you." The idea may seem far-fetched, but scientists have known for centuries that individuals have unique ways of walking, and in recent years the U.S.

Department of Defense has been funding millions of dollars of gait research, as has the Chinese government.

GM developing Wi - Fi pedestrian detection technology

General Motors researchers are developing a promising driver assistance feature potentially capable of detecting pedestrians and bicyclists on congested streets or in poor visibility conditions before the driver notices them. The feature relies on Wi- Fi Direct, the peer-to- peer wireless standard that allows devices like some smartphones to communicate directly with each other rather than through a shared access point like a cell phone tower. GM researchers have determined Wi-Fi Direct can be integrated with other sensor-based object detection and driver alert systems already available on production vehicles to help detect pedestrians and bicyclists carrying smartphones equipped with Wi-Fi Direct.

The automaker also is looking to develop a complementary app for Wi-Fi Direct-capable smartphones that can be down loaded by frequent road users such as "bike messenger" or "construction worker" that will help Wi-Fi Direct-equipped vehicles identify them. Wireless pedestrian detection is part of GM's ongoing development of vehicle-to-infrastructure (V21) and vehicle-to-vehicle (V2V) communication systems that could provide advance warning about hazards such as slowed or stalled vehicles, slippery roads or intersections and stop signs.

"This new wireless capability could warn drivers about pedestrians who might be stepping into the roadway from behind a parked vehicle, or bicyclists who are riding in the car's blind spot," said Nady Boules, GM Global R&D director of the Electrical and Control Systems Research Lab. "Wi-Fi Direct has the potential to become an integral part of the comprehensive driver assistance systems we offer on many of our Chevrolet, Cadillac, Buick and GMC vehicles."

By eliminating the intermediate step required to reach a cell phone tower, Wi-Fi Direct allows devices to connect in approximately one second compared to conventional wireless systems that typically need seven or eight seconds to acquire location information and connect.

"Wi-Fi Direct's fast connections offer a distinct advantage in vehicle applications," said Donald Grimm, GM Global R&D senior researcher of perception and vehicle control systems. "The quicker a vehicle can detect other Wi-Fi Direct users, the greater the potential for collision avoidance." The Wi-Fi Alliance, the global industry association in charge of certifying wireless standards, claims Wi-Fi Direct devices can reach each other at a maximum distance of 656 feet or more than two football fields away. In addition to aiding pedestrian detection, this range could enable secure transfers of files such as MP3s or digital address book information between a home computer and the user's Wi-Fi Direct- equipped vehicle infotainment or navigation system

---

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

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!