International Council For Industrial Security & Safety Management

Newsletter: October 2011

Let's professionalize the professionals...

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

Wish all our readers a very Happy and Healthy Diwali!

Hope it brings prosperity, pleasure and poise all year round!!

May it be safe & secure to all!

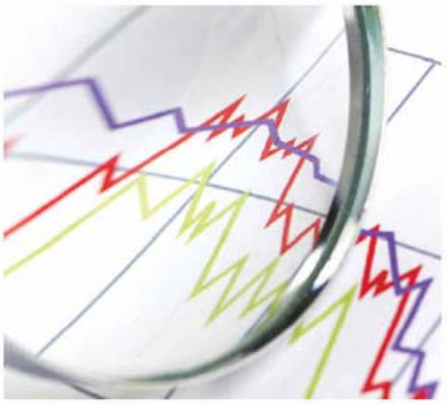
In India the season of gaiety and festivity has already begun starting with Ganesh Puja, Id-ul-fitr, Durga Puja and Dussahara! Children have been anxious and exited over the year for this period only. Dipawali is round the corner. Many families will travel to their native places leaving behind their homes locked and under the care of security personnel who have to prove themselves once again worthy of trust and confidence which such families have in them. Let all security personnel rise to this moment and discharge the duties more diligently and carefully!

However as it has often been said, security is not the duty of the security personnel alone. Everyone has to be security conscious and must discharge the basic responsibility to start living securely. In this direction, the least every one of us has to do is to secure the doors and windows while leaving the house. We keep lots of valuable items in the home and trust the security with a cheap lock! The doors sturdiness as much as heavy duty locks and bolts will add to the security of every residence.

Children need to be advised for safety precautions with fire crackers. Parental guidance is always essential and keeping first aid box is no a bad idea at all!!

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.



Emerging Security Trends

The nature of world-wide espionage is currently experiencing a dramatic shift. A recent analysis of trends suggests the need to redefine the problem and to develop new strategies to combat growing threats to national security from economic intelligence gathering and corporate espionage. If left unchecked, analysts estimate losses could grow an additional 50% by the year the next year.

A New National Security Perspective

The rapid pace of change in the post-Cold War era demands a new definition of national security issues. The development of the European Community, break-up of the Soviet Union, economic and political shifts within the former Warsaw Pact nations, the reunification of Germany, and the brisk economic growth of Pacific Rim countries have led to a new world of opportunity and threat.

The challenge to the intelligence community is to discern and disrupt economic espionage directed towards national companies and interests. A fundamental shift in our understanding and protection of the nation's secrets will require:

- Redefining the concept of national security secrets and moving beyond protection of the defense industry to assisting the entire private sector in combating corporate espionage.
- More explicitly connecting the impact of industrial espionage on the national economy to national security issues.
- Broadening the role of personnel security in non-defense industries, including a new perspective on "clearances," training, and threat awareness.
- Providing more information to the corporate community from the intelligence community regarding espionage threats, source countries, and targets and means.
- Aggressively prosecuting those involved in illegal economic and competitive intelligence.

Emerging Espionage Targets

Every industry and every country has important economic resources which must be protected. Generally, the focus of economic espionage activities can be broken down into two broad categories.

The first is formulae, processes, components, structure, characteristics, and applications of new technologies. Examples include:

- Fifth generation computer architecture; new computer chip designs, conductivity, and biochip research; and software development.
- Biotechnology.
- Supercomputing and superconductivity.
- Holographic and laser research, applications, and modeling.

- Optics and fiber optics technology.
- Aerospace technologies.
- Medical technologies, including pharmaceuticals.
- Advanced communications technologies and processes.
- Advances in satellite usage and space technologies and applications.
- Electromechanical products and technologies.
- Chemical process technology and research.
- Integrated circuit technologies.

The second category is factors associated with the marketing, production, and security of new technologies. Examples include:

- Pricing information.
- Marketing research on demand and consumer profiles.
- Products needed for compatibility and applicability.
- Production timetables and product release dates.
- Production quantities.
- Market targets and schedules and overseas marketing plans.
- Security equipment, sensors, and processes.
- Electronic banking equipment, interfaces, and protocols.
- Technology-upgrade schedules and planned changes in technology.
- Software developments, especially those enhancing new technologies, networking, and technological integration.

Two Vulnerable Targets: Computers and Intellectual Property

Computers provide both a target and a tool for industrial espionage. The new information highways provided by network systems (like Internet, Milnet, and Bitnet) and other advances like Electronic Data Exchange (EDI) and SWIFT (Society for World International Financial Transactions) also can mean increased access for illegitimate purposes. Computer-related crimes can be broken down into four main categories.

Computers as Targets: This relates to unlawful accessing of computers to gain information or to damage programs or hardware. A wide array of crimes fall into this category including: theft of intellectual property or marketing information, blackmail, sabotage of files, accessing and/or changing government records, techno-vandalism (causing internal damage to computer systems) and techno-trespass (violating the privacy of computer files).

- **Computers as Crime Instruments:** Computer processes used as instruments of crime. Examples include: ATM fraud, rounding off monetary entries, credit card fraud, fraudulent computer transactions, and telecommunications fraud.
- **Incidental Criminal Computer Use:** Computers used to increase the efficiency of traditional crimes, for example: money laundering, off-shore banking, pedophile information exchanges, organized crime record keeping, murder (through changing information in hospital records or other control systems), and bookmaking.

- **Crimes Associated With Computer Prevalence:** The advent of microcomputers has opened new crime and espionage targets. These include: software piracy/counterfeiting, copyright violations, counterfeit and black market computer equipment and programs.

Another growing target of economic / industrial espionage is intellectual property. It consists of concepts, ideas, planning documents, designs, formulae, and other materials intended for products or services which have commercial value and represent original thought or work. It may be clearly protected (with copyrights, trade-marks, patents, or as trade secrets) or less well defined (in the case of non-protected research, incomplete new concepts or ideas, and public domain information which has been individually modified or refined).

Intellectual property is increasingly sought through industrial espionage because it can reflect a valuable investment involving lengthy research and development efforts. Moreover, it is often stored on computer media which are them-selves an increasing target of espionage.

Methods of Espionage

In addition to unlawful computer access, many of the traditional methods employed in national security and industrial espionage will continue to be prominent. Among the many means of obtaining information are:

- Open sources (Right to Information Act requests, published government documents and bidding specifications, opened bids and technical journals).
- Consultants or outsourcing contractors from targeted firms who provide "inside information" to competitors.
- "Moles" working inside a particular industry or company with access to desired information.
- Computer hacking and data transmission interruption.
- Compromising employees through blackmail, set ups, corruption, and bribery.
- The use of student researchers and interns to gain access to research.
- Surveillance of corporate employees.
- Intercepting communications through faxes, telephones, etc.
- Burglary.
- Gaining access to records through janitorial or service personnel.
- New technologies and techniques adapted as detection devices or espionage countermeasures.

Motivations for Espionage

In general, the primary motivation for engaging in espionage is monetary. However, several factors have emerged in recent years that may make it easier for employees or others to participate in economic espionage. As espionage activity has shifted away from a focus on

national security, the profitability of spying has increased. In addition, economic espionage (especially when information is divulged to traditional national allies) is less morally repulsive than betraying a national security secret and does not incur the same threat of punishment.

Employers should watch for a number of key characteristics that may indicate a security risk. Security threats may include employees who:

- Are generally unhappy on the job, or unhappy with the location of their assignment.
- Believe they have been overlooked for promotion, salary increases, or commendations and rewards.
- Feel their contributions to the company are ignored and uncompensated.
- Are facing personal financial difficulties.
- Have personal problems.

Prevention

There are a number of measures that employers can take to reduce industrial espionage. The most crucial of these are related to effective personnel policies and procedures.

Selection: Employees should be recruited and screened on the basis of their knowledge, competence, loyalty, and psychological and social stability.

Training: Employee training should include information about security threats and procedures.

Surveillance: Maintaining control over and limiting access to sensitive information will reduce potential losses.

Supervision: Attentive supervisors can both identify security violations as well as intervene before problems occur by remaining alert to warning signals.

Accountability: Ensuring that employees follow procedures, perform efficiently, and adhere to organizational values will help maintain personnel integrity.

Target Hardening: Measures should be taken to protect crucial information and to improve security in order to reduce temptation.

Positive Work Environment: Increasing employees' sense of worth within the organization can increase their sense of obligation and loyalty, thereby decreasing the possibility of espionage.

Realistic Sanctions: Employees must have a realistic sense that security violations will be identified and severely punished.

Positive Rewards: To balance the threat of discipline, positive contributions to the organization must be reinforced and rewarded.

Reinforcement of Ethics and Values: The organization must strengthen its employees' sense of moral obligation through a statement of organizational values, reinforcement of ethical standards, and high standards of professionalism.

A bit of adhesive is all that's needed to steal from ATM

Beware if the ATM screen goes blank after you swipe your card. It could be a mischief by fraudsters to withdraw cash from your account after you leave the ATM in a huff. A bit of adhesive and a screwdriver are all that's needed to outwit hi-tech safety gadgets.

These swindlers are part of a powerful inter-state network spread across the country. Assam Police and Kolkata Police have recently rounded up three swindlers who have mastered the tampering of ATMs.

The trick applies only to ATM machines that need a customer to insert and extract the card to start operations (as opposed to ATMs where the card pops out after the transaction is complete). Many nationalized banks, including State Bank of India (SBI) and Bank of Baroda, use this system at their ATMs, most of which are unmanned.

So, what is this low-tech, highly effective modus operandi? Fraudsters, who generally strike in pairs, enter ATM by swiping valid debit card at the gate, press down a key on keyboard and stick it with adhesive so that it does not return to its original position. This switches on the machine. They then walk out and wait for a victim to step into the trap!

When a customer enters the ATM and swipes the card, he does not realize that the machine is already on. A message flashes for him to key his PIN, which he does. But since the machine has been switched on in an improper way, the screen goes blank automatically as a security feature to stop fraudulent withdrawals.

The customer thinks it is a system fault and gives it a second try. He has no clue that the two 'customers' getting impatient outside are actually criminals waiting to steal his money. They start abusing him for taking too much time and force him to leave in a huff. Exit customer, enter fraudster. They simply use a screwdriver to 'release' the key. The ATM restarts automatically. What it has in store is PIN of the last customer who swiped his card. The gang enters the amount and walks out with cash.

The SBI has been receiving several such complaints. "We were at a loss to locate the fraud because the CCTVs showed the customer swiping his card. But customers complained that they couldn't withdraw money," an SBI official said.

Webcams can be hijacked by Trojan Technique!!

By: Col R K Mishra, COAC' CC*

A new worm has been discovered in the wild that's not just settling for invading users' PCs--it wants to invade their homes, too.

The Rbot-GR virus follows a fairly traditional malware route of exploiting Microsoft security vulnerabilities and installing a Trojan horse on infected machines. However, the worm also spies on users by taking control of their Webcam and microphone, then sending images and soundtracks back to the hackers, according to antivirus firm Sophos.

As well as getting an insight into homes and businesses across the world, the worm allows the malware writer to take a look at information on the infected machine's hard drive, steal passwords and launch denial-of-service attacks.

Graham Cluley, senior technology consultant at Sophos, said the virus could be used for industrial espionage--or simply by a nosey hacker to take a look into people's bedrooms. "Whether this worm is the work of professional snoopers or lusty teenagers--it's hard to say for certain," Cluley said.

"What we do know is that there have been a few hundred different versions of the Rbot worm, all of which have been designed to gain some kind of remote access to innocent users' data. This one goes further by also specifically collecting Webcam footage. It seems more and more hackers are building a cocktail of different functionality into their creations."

Those who have the virus may be unaware that their every move could be being tracked by remote hackers. An infected Webcam may show an "active light" when it's being used, but Webcams without such light would offer no giveaway the hacker is watching.

About the author

An avid reader and equally prolific writer, Col Ram Kishore Mishra is Management Professional possessing outstanding leadership qualities with 27 years of well-honed expertise and cross functional experience.

Hand-picked by Army Headquarters to Command an Assam Rifles Battalion and launch them into high intensity counter insurgency combat zone (OP HIFAZAT).

He also ensured complete domination of area of responsibility over rugged mountains of North J&K along line of control under (OP RAKSHAK).

He is recipient of Chief of the Army Staff's Commendation for gallantry beside Commendation of General Officer Commanding in Chief, Southern Command for devotion to duty and distinguished service

He can be contacted at rkmishra58@gmail.com

There is, however, one simple way to dodge the prying eyes of the malware merchants--just unplug or switch the Webcam off when it's not in use.

Now that's just plain spooky...

…..throw towel over webcam

Feedback

From: Raghubir Singh [mailto:raghubirs@gmail.com]
Sent: 08 October 2011 15:11
To: Corporate Security Department
Cc: Capt. S B Tyagi;
Subject: Re: ICISS Newsletter Oct.11

Dear Capt SB Tyagi,

I am sure in times to come Private Security will acquire the dimensions of corporate business which it amply deserves. Seeing dishevelled , poorly paid with over stretched duty hours, ill-trained people put on security duties with merely a crumpled uniform signifying his role-I ventured out to make a Diploma course under the aegis of Annamalai University last year. The details of the course is available on www.snehaamu.com-I am sending you excerpts.

I am not in the business of education but have given this info only to show my linkage with Security. There would be occasion to improve the syllabus & make it more broad based by including topics like how to prevent Bank robbery as I read in your well brought out newsletter.

We have to improve social awareness about security which should be paramount in our day to day life-in homes, offices, public/religious places etc. Not only roads even skies too are not safe & require security as never before. You professionals in the field have to make efforts to contribute in this regard.

Air Cmde Raghubir Singh (Retd.), Pune

DIPLOMA COURSE FOR SECURITY SUPERVISORS : CODE:729

Medium: English
Duration: One Year
Eligibility: Candidates for admission to one year Diploma Course for Security Supervisors should have passed 12th or equivalent examination.

1. Concept of Security
2. Uniform & PSAR Act / Rule of 2005
3. Leadership for Security
4. Disaster Management

Air Cmde Raghubir Singh (Retd) Tech. Advisor
Bc (Engg) Mech, MSc (Def), ME (Aerospace Engg) FIE, FAeSI, FIETE, C Eng
He has served in the Indian Air Force in various capacity, in DTE of Technical Development & Production(Air), HAL on Mig-21 & Missiles inspection & has also served in the Defence Research on frontier areas of technology. After his retirement, he has been actively involved in education field.

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!