International Council For Industrial Security & Safety Management

Newsletter: Sept 2014

Let's professionalize the professionals…

http://sbtyagi.wix.com/icissm

Best Practices to Maximize Performance In Security Industry

State of Industrial Security

Market competition in industry has traditionally driven the evolution of control systems – physical as well as network and virtual! Over a decade ago, most control systems were autonomous and built upon proprietary vendor technology and the solutions were geared towards access to personal, data, processing speed, and functionality (or reliability). The most important feature was access to data. At first many vendors built their own protocols or languages to allow for the transfer of data and soon the automation landscape became very proprietary and independent of other systems and protocols. Parallel to this was the development of Ethernet networks for business data networks. In early 2000, vendors saw advantages to include 'Ethernet-compliance' to allow for communication between security systems including those outside the plant environment. However, in the rush to market many vendors built ad-hoc versions of protocols that worked for the purpose at hand but did not include security.

Now most industries with control systems are facing many pressures to both allow access to data and personnel and to secure them. There are many forces pushing these opposing trends including data access to enable business decisions, vendor access for process improvements and advanced control exercises like loop tuning and alarm management. However this increasing need for access is further diluting the security of many of these systems and is putting many process control environments at risk. In some industries this is more of a nuisance than anything, but for most industries a loss of control over your process can mean a serious safety threat.

As one noted security professional who works for a major refinery once pointed out, "our industry is one such that a loss of access or control over our systems usually means someone dies". Regardless of the potential harm, any industry with little or no security in and around their control system will at least lose production for some time. This can translate into re-work, overtime, environmental release, and other intangibles such as competitive edge, investor confidence and potentially the ability to stay in business.

The new push for control systems is to try to balance the two opposing trends: Access and Security. And the pressure is coming from many angles. Increasing market competition means that most industries are 'pushing the envelope' to run faster, more efficiently and with less downtime. This means more outside 'tuning' and better visibility into production from specialized experts who may not be physically at the site. The advancing age of the workforce in general means many

industries are automating more control of their assets and expecting the same staff to manage & optimize more resources thereby increasing their reliance on computers.

Security Pacesetters – What are they doing?

The scope of the term 'security' often seems vague and the sheer volume of effort and areas of concern this may represent can be overwhelming. However, this need not be the case. In looking at a number of security frameworks or standards a common theme emerges that is quickly being adopted as a holistic and effective approach to security. This approach combines efforts and initiatives that go far beyond the purchase and deployment of technology. Different initiatives offer different sections, headings and names for each of their areas of concentration but in the end, all efforts can usually be summed into three (3) foundational areas: People, Processes and Technology. The priority of developing a security philosophy is needed in essence which will in turn foster a security culture.

Before beginning any security program or initiative your organization must first adopt a security philosophy. A security philosophy will sound different for each company, industry and region in which it is created but there are some basic requirements that all security philosophies must have.

Underpinning all efforts within organizations one must first have a security philosophy and always work towards creating and maintaining a strong security culture or your momentum will be lost. What we call security surveys and security audits are basically 'outsourced introspections'! Such exercises are required to focus on following areas -

- What are the policies and standards we currently have?
- How well are they implemented?
- What issues / problems do we have?
- What requirements apply to our industry?
- Where do we need to be from a security perspective?
- How will we change / improve the situation?

Caveat emptor – Understand what you're buying into

There is no "standard" standard. It is not a cliché. In fact there are no set standards in India so far as security systems and gadgets are concerned. There are no governing / regulatory bodies and industry itself has failed to develop its own self-regulatory mechanism as developed by films industry, broadcasting and media industry or the IT Education Industry. In UK BISA is watchdog which sets standards for security guards, supervisors, pub bouncers, front man etc. BISA is also setting the training and education standards for security personnel. Similar initiatives are undertaken by ASIS in USA.

Knowing which standard to choose and what your obligations are as a result of that choice, is key first step in managing compliance. Some industries and organizations are required to meet security standards established by laws or regulations. While buying the security systems or gadgets, security professionals need to first understand the technology and also what can be done with it including its limitations. The shelf life of a system or gadget is directly related to its technology – which is changing very fast. Today what is current and 'the thing', may not be

maintainable / repairable in a very short time. A system must have longevity of at least 6-10 years with on-site repair condition. ***Thinking that technology can solve all the problems means that either you do not understand the technology or you do not understand the problem!***

Security is Important

The first premise is quite simply that security is important to the organization. This means the decision makers, the owners and operators of the systems, the support staff, the consultants, vendors, site staff, in short everyone, understands that keeping your facility secure is in everyone's best interest. This is no different from the importance placed on safety.

More often than not, an industrial facility has a long history of always trying to raise safety awareness and tried to educate everyone as to why safety is important. Every employee, contractor and visitor onsite needs to have safety orientation and updated each year. This also needs to happen for security, and can be integrated into safety programs. Without rank and file team members who understand their role and the importance of their actions (or inaction) at your site, you will not succeed in securing your facility. It is a harsh reality but the simple fact remains that your internal, trusted employees have the greatest opportunity to cause or create a security breach intentionally or otherwise. In other words, ***your security program is only as effective as your least informed employee.***

Security is On-Going

More often than not, many organizations see security programs or initiatives as projects that have a defined start, finish and cost. This may be the case for a particular component of your on-going security efforts, but true, lasting security is an on-going initiative. This is quite simply due to the fact that security concerns are brought about by technology - and technology keeps changing! What was a threat yesterday or last week may be fixed by your current security plans, but the next threat coming will not be as deterred. Less than 5 years ago USB keys or 'thumb drives' were an emerging fad. Today they are sold more cheaply than ever, are capable of huge storage capacities and require little or no knowledge of specialized applications or programs for using them. This was not a concern a few years ago. ***Unfortunately your security program is only as effective as it is current***.

Security is Everyone's Concern

This topic is the basic premise on which your security philosophy needs to be built. As mentioned earlier, your weakest link and biggest threat is your least educated employee. If you install security programs, risk management processes and a healthy business continuity plan or disaster recovery plan you are well on your way to securing your environment. However, if any of those efforts cause a change in the day-to-day business flow for your employees then you will need to explain to them why these changes are necessary. Too many times are programs implemented without the proper awareness training and education for the people whose daily lives are most affected? In these cases it is only a short time before the day-to-day users start to find ways around the new systems you just put in place thus negating your efforts. Think of a school computer lab where students are some of the most creative people at bypassing security because they do not understand or care about security. ***Your security program will live and die based on how well your employees receive and embrace it.***

Security is a Balancing Act

The last and perhaps most important thing a proper security philosophy needs is the attitude of balance. In this sense the balance is between risk and reward as well as between effort and return. In order for your organization to move toward a proper security program you must first decide as an organization what level of risk you are willing to live with. Every change you make to your current environment towards security is going to cost something whether it is time, money, or access to your data. And no matter how you do proceed, there is a very good chance that you will still have some sort of incident at some point in time.

A security incident can be catastrophic system failure, accident in process area or subtle inappropriate access to data or an IO room. The true measure of your security program will be in how well contained the incident is, how quickly you recover, and if you choose to learn and benefit from it.

Prepare for exceptions

The day will come when a business need conflicts with a security best practices. Being prepared to deal with this situation will save time, money and aggravation.

Every business has different needs and tolerance for risk. At some point, business needs may win out over security best practices. You need to have a process in place to allow the organization to:

- Understand the risks being taken
- Document these risks and their mitigating factors
- Make and document an informed decision as to whether to accept a risk
- Periodically review accepted risks to determine whether new mitigations are available and whether the risk is still acceptable

Having a well-defined process to handle exceptions will allow your organization to deal with situations that fall outside of those anticipated when the policies were written.

Translate standards into measurable actions

Hand your business managers a copy of typical standards and they'll probably end up using them – to prop up the short leg on the table in the break room.

Business unit folks want security folks to provide them with specific instructions on how to make their systems and premises secure. Telling a business unit manager to "use two-factor authentication to protect critical information" or to tell them to “use ACS along with IDS on common platform” is not helpful. You need to provide your users with organization-specific tools, such as criteria for deciding whether information / facility is critical or not, and lists of tested and approved security solutions specifically tied to policies.

Remember, policies are not instruction manuals. Policies are high-level statements of the intent of the organization. Specific information as to how to implement policy should be laid out in procedural documents. The key here is clarity and consistency. You should be able to put the

same procedural and policy documents in front of everyone in your organization and have them come to the same conclusions as to the security measures that are needed to meet the standard.

If your organization has an Internal Audit department, these are good people to get involved in the process of developing measurable actions. After all, they will be doing the measuring of compliance, and their experience in other types of audits and standards is a valuable resource. Auditors have the structured approach needed to put this practice to work. If our friends in Washington or your state capital dictate your external standards, get your legal folks involved as well to insure that your measurements will hold up in court.

Industry standards for security are not a cure all – and this is a good thing on the whole. While legislators and industry groups can tell us a lot about best practices and goals, it is up to the management and security professionals in our organizations to come up with the processes and procedures.

Security Professionals Need Education

Education remains an area of concern for security professionals. The perception is that professionals with army or police services are inadequately prepared to create secure environment and premises. One comment seemed to resonate with many: “If it’s fair to expect a journalism graduate to write with appropriate grammar, why can’t we expect ex-army / police officers to plan and execute good security measures?”

This problem arises from a number of challenges, particularly the need to adjust curricula to meet the ever-changing technology landscape. Security is also an “eat your vegetables” topic that most security professionals rank low on their hierarchy of interests. The onus falls to employers and groups like ICISS / IPSA / BISA / ASIS / SAFE Code to inform training institutions of the need for candidates who are well trained in how to plan, execute and revise / review the effective security plans as per changing needs of varied organizations and industries that allow business to be conducted with assurance.

Security is part of productivity and profitability

Security is treated in most business and organizations as ‘cost center’ needing budgets for non-productive systems and plans. Security is also seen as burden which is evil yet essential. There are issues such as insurance, legal compliances, pressure from stakeholders etc. that meager budget is allocated to security department. Mostly security professionals are to be blamed for this misconception.

It is good security that guarantees secured, hassle-free congenial work atmosphere where all production, operation and maintenance or marketing activities are conducted smoothly without fear or danger. No one can work; forget the best performance, if there are chances of attack by miscreants, theft of costly inventory or law-and –order problems inside the premises or at work-floor areas.

Good security means good production, means higher profit!

Changing Scenario: Security Services In India

Digital displays changed the approach of modern man towards time and especially towards wrist watches. Hitherto, time was seen but suddenly time was being read with digital watches. So, analog watches were replaced by digital watches even when for a short time. Since the need for analog watches remained and technology transition took time, a new genre of watches, called “Digi-ana” (Digital and Analog) was brought to the market.

Similar technology driven changes were made in banking industry which greatly facilitated customers and also impacted security concerns. ATMs changed the ways banking is done! Since banks wanted to cut operational costs, they also wanted less and less customers coming to their branches for mundane banking activities such as cash withdrawal, balance inquiry or pass-book updates. ATMs were answer to all such needs and were found to be convenient, efficient and low cost. As Customers liked it, banks eagerly multiplied the number of ATM’s. Initially different group of credit cards were present, soon debit cards also joined the hustle-and-bustle and soon majority of ATM’s started accepting all leading brands of credits cards and debit cards of all leading banks. At this stage since foot falls per ATM increased, increased need of cash in ATM caused security concerns. The licensing authorities, regulators and police demanded effective security measures for ATMs, causing increased administration costs. Thus ‘banking-away-from banks’ became expensive propositions considering 24x7 operation and security needs.

It is well studied forecast of changing trends in ATM operations that soon ATMs will remain just ATM without carrying name of any bank. All the transactions using credit / debit cards will carry transaction fees and operation and maintenance will be by some specialized agency other than the banks. Thus ATM operations will cater to varied needs of the customers and also incorporate directives of the regulator, licensor and the police. It is further envisaged that soon in India every citizen will have only one bank account against the present freedom of holding multiple accounts in multiple banks. This migration to ‘regulated bank account regime’ will go long way for effective e-governance and reducing black money as well as reducing tax thefts.

In this emerging scenario; changing trends in security management will develop. Two major trends are foreseen-

- **Central Command & Control Centre**
- **ATM Management Services.**

There have been pioneering services started by few leading companies in Metro cities where under command and control center have been established by them with the trained manpower and sufficient resources with Quick Response Teams, to take care of specific need of clients.

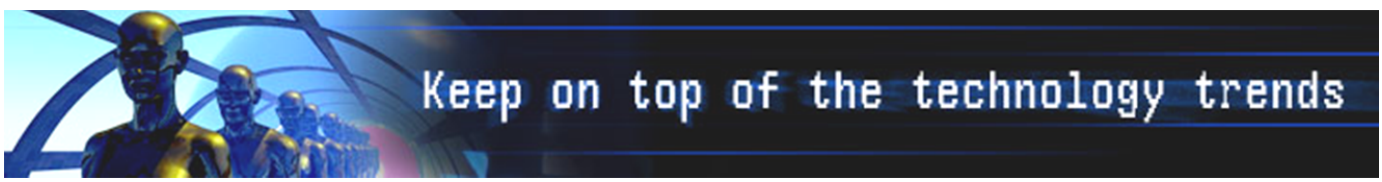
The clients' CCTV and other alarm system are maintained and monitored, notifying the pre-identified authorities, mobilizing the resources to mitigate the alarm situation and prepare post-event reports. Since this area of specialized service has just opened-up, there are not very many players and standards are non-existent.

So far as ATM Management Services are concerned, the direction and decision of the Government will decide the shape this segment is to take. Early indications are that Central Government is seriously thinking of providing a bank account to every citizen of India linked with Aadhar and or National Citizenship Card.

The citizen will have a choice for selecting a bank. Electronic transactions will be favored or rather encouraged. Instead of going to the banks, the customer would be led to ATMs where any type of card from any bank will be acceptable. For each transaction the concerned bank will charge fees from customers, part of which will go to franchisee running / maintaining the ATMs.

Thus new service segment will emerge which will offer range of services including congenial and secured environment where customer would prefer to have ATM transaction, cash transportation to feed ATMs, security of machines and the facilities and up keep and maintenance of ATMs. All the gamut of services related to ATMs will be preferred to be provides by one services provider.

Thus, it can be seen by above that soon there will be two specialized services sectors emergency in broad area of security management for which niche is already created. Some pioneer work has already been done and industries thought-leaders have already begun the initiation to shape-up this segment further.



UK Airports on Alert over Smartphone 'Bombs'

London: Al-Qaida terrorists have found a way to turn smartphones – especially iPhones and Samsung Galaxy handsets – into explosive devices and intend to explode them on commercial flights, it emerged on Friday. Britain has tightened security in airports across the UK after receiving credible evidence from US of a "possible al-Qaida terror".

The threat is "Different and more disturbing" than previously attempted techniques including explosives hidden in toothpaste, shoes and ink cartridges. US officials said that smartphones will be used as 'stealth bombs'. UK has also been informed that explosive makers from Yemen-based al-Qaida have discovered how to turn the phones into explosive devices which are extremely difficult to detect. British airports, including Heathrow and Gatwick, have now decided to put in a second layer of checks at departure gates.

The key suspect is Syria based Jabhat al-Nusra, who has joined hands with members of al-Qaida in Yemen.

A mini-cam to scan crowds for Suicide Bombers?

Beijing: Chinese scientists have developed a mini-camera can scan the crowd for highly stressed individuals, in a bid to prevent suicide bombing, media reports said on Tuesday. A research team led by Chen Tong, associate professor at South West University in Chongqing developed a 'stress sensor' that can help the police to spot suicide bombers by capturing the stress levels of people, Hong Kong-based South China Morning Post reported. "The sensor measures the amount of oxygen in blood across exposed areas of a body, such as the face. The higher the mental stress, the higher the blood oxygenation," it said.

"The readings of the device may not be always reliable. For example, with enough practice, a person can learn to control their heartbeat," the report added. The technology comes amid heightened fears the country witnessed brazen terror attacks by native Uygur separatists in the northwestern Xinjiang region recently.

Talking about the functionality of the device, Chen said that "officers looking through the device at a crowd would see a mental 'stress bar' above each person's head and the suspects highlighted with a red face". "Laboratory tests of the technology had yielded encouraging results," Chen added.
