International Council For Industrial Security & Safety Management

Newsletter: January 2013

Let's professionalize the professionals...

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

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.

Capt S B Tyagi
For ICISS

With the fond hope and firm resolve that the coming year
Will be harbinger of peace and love,
Let us wish every law-abiding citizen
A Happy and Prosperous New Year!

Make Security a thing to remember,
From January till December!

Best Practices to Maximize Performance In Security Industry

Introduction: 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 / ISSM / IPSA / CAPSI / 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. PSAR Act 2005 attampts very feebly to lay down training standards for security personnle but fall short of desired details.

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!***

Ways to build physical security into a Computer / data center / server room

At giant companies, data centers don't just hold the crown jewels; they are the crown jewels. Protecting them is a job for security officers, of course. But just as important, it's a job for those with expertise in physical security and business continuity. That's because all the encryption and live backups in the world are a waste of money if someone can walk right into the data center with a pocket knife, a camera phone and bad intentions.

There are plenty of complicated documents that can guide companies through the process of designing a secure data center-But what should be the CSO's high-level goals for making sure that security for the new data center is built into the designs, instead of being an expensive or ineffectual afterthought?

Read below to find out how a data center is designed to withstand everything from corporate espionage to terrorists to natural disasters. Sure, the extra precautions can be expensive. But they're simply part of the cost of building a secure facility that also can keep humming through disasters.

Build on the right spot. Be sure the building is some distance from headquarters (20 miles is typical) and at least 100 feet from the main road. Bad neighbors: airports, chemical facilities, power plants. Bad news: earthquake fault lines and areas prone to hurricanes and floods. And scrap the "data center" sign.

Have redundant utilities. Data centers need two sources for utilities, such as electricity, water, voice and data. Trace electricity sources back to two separate substations and water back to two different main lines. Lines should be underground and should come into different areas of the building, with water separate from other utilities. Use the data center's anticipated power usage as leverage for getting the electric company to accommodate the building's special needs.

Pay attention to walls. Foot-thick concrete is a cheap and effective barrier against the elements and explosive devices.

Avoid windows. Think warehouse, not office building! If you must have windows, limit them to the break room or administrative area, and use bomb-resistant laminated glass.

Use landscaping for protection. Trees, boulders and gulley can hide the building from passing cars, obscure security devices (like fences), and also help keep vehicles from getting too close.

Use retractable crash barriers at vehicle entry points. Control access to the parking lot and loading dock with a staffed guard station. Use a raised gate and a green light as visual cues that the bollards are down and the driver can go forward. In situations when extra security is needed, have the barriers lift-up by default, and lowered only when someone has permission to pass through.

Plan for bomb detection. For data centers that are especially sensitive or likely targets, have guards use mirrors to check underneath vehicles for explosives, or provide portable bomb-sniffing devices. You can respond to a raised threat by increasing the number of vehicles you check—perhaps by checking employee vehicles as well as visitors and delivery trucks.

Limit entry points. Control access to the building by establishing one main entrance, plus a back one for the loading dock. This keeps costs down too. Make fire doors exit only. For exits required by fire codes, install doors that don't have handles on the outside. When any of these doors is opened, a loud alarm should sound and trigger a response from the security command center. Use plenty of cameras. Surveillance cameras should be installed around the perimeter of the building, at all entrances and exits, and at every access point throughout the building. A combination of motion-detection devices, low-light cameras, pan-tilt-zoom cameras and standard fixed cameras is ideal. Footage should be digitally recorded and stored offsite.

Protect the building's machinery. Keep the mechanical area of the building, which houses environmental systems and uninterruptible power supplies, strictly off limits. If generators are outside, use concrete walls to secure the area. For both areas, make sure all contractors and repair crews are accompanied by an employee at all times.

Plan for secure air-handling. Make sure the heating, ventilating and air-conditioning systems can be set to re circulate air rather than drawing in air from the outside. This could help protect people and equipment if there were some kind of biological or chemical attack or heavy smoke spreading from a nearby fire. For added security, put devices in place to monitor the air for chemical, biological or radiological contaminant.

Ensure nothing can hide in the walls and ceilings. In secure areas of the data center, make sure internal walls run from the slab ceiling all the way to sub flooring where wiring is typically housed. Also make sure drop-down ceilings don't provide hidden access points.

Use two-factor authentication. Biometric identification is becoming standard for access to sensitive areas of data centers, with hand geometry or fingerprint scanners usually considered less invasive than retinal scanning. In other areas, you may be able to get away with less-expensive access cards.

Harden the core with security layers. Anyone entering the most secure part of the data center will have been authenticated at least three times, including:

- At the outer door. Don't forget you'll need a way for visitors to buzz the front desk.
- At the inner door. Separates visitor area from general employee area.
- At the entrance to the "data" part of the data center. Typically, this is the layer that has the strictest "positive control," meaning no piggybacking allowed. For implementation, you have two options:
- At the door to an individual computer processing room. This is for the room where actual servers, mainframes or other critical IT equipment is located. Provide access only on an as-needed basis, and segment these rooms as much as possible in order to control and track access.

Watch the exits too. Monitor entrance and exit—not only for the main facility but for more sensitive areas of the facility as well. It'll help you keep track of who was where when. It also helps with building evacuation if there's a fire. Prohibit food in the computer rooms. Provide a common area where people can eat without getting food on computer equipment.

Visitor's rest rooms. Make sure to include bathrooms for use by visitors and delivery people who don't have access to the secure parts of the building.

The leadership Principle:

As soon as the fear approaches near, attack and destroy it. Secure you must, all your interests! - Chanakya, the Great Strategist

Get Your Mobile 'Immunized'

Those intrusive and unwelcome mobile viruses and spam-What can Indian mobile operators do? Check out the solutions and problems

Rapidly expanding mobile phone industry has already over three billion mobile subscribers worldwide [Source: ABI Research: Mobile Subscriber]. This is largely contributed by countries such as India, where mobile phones are the prevalent form of communication, as many people are unable to gain reliable access to landline telephony, and mobiles provide a cheap and easy way of staying in touch. Whilst this is very positive for operators' revenues, the requirement for keeping their networks clear of spam and viruses is absolutely paramount, as consumers put their trust in reliability and accessibility, and are often left frustrated when services fall short of expectations. According to the International Telecommunication Union (ITU), more than 80% of mobile phone users worldwide have received an unsolicited message on their handset at some point. The hidden motive behind such messages is often to lure the subscriber into calling a premium rate number to buy a product or enter a competition. Messages are commonly not commercially focused, and in some cases can be deemed offensive, but all have one thing in common: they are intrusive and unwelcome.

Problems

It is rare for a mobile user not to have received an unsolicited mobile spam message in the form of a text message (SMS), picture message (MMS), or video message (VMS). Whilst it is standard to have spam filters on emails when using a home computer, personal and corporate mobiles that feature Internet and email access are extremely vulnerable to mobile spam. In fact, users are completely dependent on their mobile network operator to manage these unwanted communications. The conflict here is that in most cases, the operator is gaining extensive revenue from the spam, which impacts on their desire to protect the subscriber. Some mobile operators around the world actively encourage spam by supplying content and application providers with their users' mobile phone numbers and the only way for a subscriber to get rid of the spam is to switch to operator. In India some operators face spam levels of about 30% [Source: Bloomberg.net, August 1st, 2008 (online)], even after protocol-level filtering.

Another concern for mobile operators is the sharp rise in mobile phone viruses, with a reported 400 in existence today. One mobile operator has noted a rise in attacks from 0.6% of all messages to 6% over the last 12 months, averaging 100,000 virus incidents per day-up from 70,000 per day only 1 year ago [Source: AdaptiveMobile]. It sees Sharp Rise in Volume of Mobile Network Virus Attacks (online). Mobile viruses are also fast becoming a menace to businesses as they move easily between handsets and infect shared address books. These viruses spread in a similar way to PC viruses, going straight to the address book and infiltrating the phones of people who accept the SMS or MMS.

Corporate phones are particularly vulnerable to the threat posed by viruses as most employees fail to check their phone bill, sending the charges straight to accountants, and won't notice suspicious increases in call charges. To add to this worry, 86% of mobile phone users have no security software installed [Source: 2008 online well-being survey, F-Secure Corporation]. We

know from our own data that subscribers whose phone do get infected can lose up to 100 Euros a day from MMS being sent from their phone by the virus.

Solutions

To prevent mobile spam and viruses becoming a problem for their subscribers, Indian network operators must ensure they don't solicit spam. Operators also need to take a leading role in the development of built-in network security to protect mobile phones, and prioritize customer satisfaction above potential ready-money revenue generated as a result of spam and viruses.

To ensure protection from mobile spam and viruses, operators must also secure their network. This way, not only known viruses, but also anomalies within the network can be detected, isolated, and disinfected, enabling network immunization. Having security on the network also means that employee-specific policies can be set. For example, an employee may not be allowed to download content which can be considered out of line from their business pursuits, while others may be prohibited from accessing the mobile Internet altogether-a similar approach to the one some organizations are already using for their PC infrastructure.

The constant evolution of spammers' techniques, combined with the continually growing mobile telephony industry, means that the battle for consumer trust is only just beginning-and mobile operators have to make sure they are competing effectively.

The last word in Airline Security?

The last word in Airline Security?

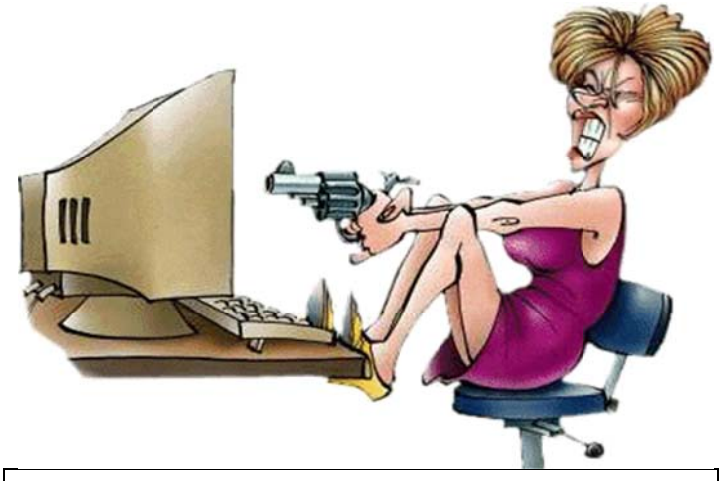
A new walk-through airport lie-detector made in Israel may prove to be the toughest challenge yet for potential hijackers or drugs smugglers. Tested in Russia, the two-stage GK-1 voice analyzer requires that passengers don headphones at a console and answer: ”Yes" or "No" into a microphone to questions about whether they are planning something illicit.

The software will almost always pick up uncontrollable tremors in the voice that give away liars or those with something to hide, say its designers at Israeli firm Nemesysco. "In our trial, 500 passengers went through the test, and then each was subjected to full traditional searches," said chief executive officer Amir Liberman. "The one person found to be planning something illegal was the one who failed our test." The GK-1 is expected to cost between $10,000 to -$30,000 when marketed. A spokesman for Moscow's Domodyedevo Airport, which is using a prototype, said "the tester (lie detector) has proved to be effective and we are in principle ready to use it". The September 11, 2001 hijacking attacks have led to a slew of innovations designed to boost airline security. Lieberman said several countries had expressed interest in the GK-I. "Unlike conventional lie detectors .such as the polygraph, this is minimally invasive, requiring hardly any physical contact," Lieberman said, adding that the first stage of the test takes between 30-75 seconds. Those that fail are taken aside for more intensive questioning and, if necessary, are searched. Lieberman said around 12 percent of passengers tend to show stress even when they have nothing to hide. "Some may feel nervous because they have used drugs, while having no intention to smuggle drugs," he said. "The whole thing is performed in a low-key manner to avoid causing anxiety." Reuters

Dates to Remember!

For more detail please contact –

Policarpia C. Secretaria Jra.
Managing Director, PCS Training Consultant
Lipata, Minglanilla, Cebu, Philippines, 6046
T: 0063-260-05-57 M: 0063-9064116749
E-mail: polly.secretaria@pcstconsultant.com,
Web: www.pcstconsultant.com



Ever had days like these??? If not, you haven't had a computer long enough.

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