Let's professionalize the professionals…

ICISS

Newsletter: December 2016

International Council for Industrial Security & Safety Management

Demonetisation in India- Myth and Reality

Sukumar Mukhopadhyay

The amount of tears that the rich have shed for the suffering of the poor for their difficulty in standing in queues in banks will easily make a vast ocean.

I went about with a friend asking many people, those in the queues in banks, and others in the market for their opinion on it. They all agreed there was inconvenience but they supported it. For they know that it will not hurt them. It will hurt only the rich will quietly take 10 0r 40 or 90 lakh rupees of cash extra along with a cheque while selling house on the ground that the buying side was insisting on it. These are all bogus claims! Is it pure and simple greed on their part? Demonetisation will hurt the doctors and lawyers and real estate agents and corrupt people in general who simply take the cash and not give a receipt. Black money shines in our society. And some of the shining writers have got black money.

All you need to know about - Demonetization in India 2016

While the suffering public has supported demonetisation, some of the economists have expressed reservation. Raghuram Rajan has said, good fiscal policy is better. He has not said why demonetisation is not advisable or why both cannot be done. Similarly Kaushik Basu has said that demonetisation is not good but he did not say why. Prabhat Patnaik has said, "...government which has embarked on an undeclared “Emergency”: it is as fatuous as it is against the people". Arun Kumar, a writer of a book on black money has sent a note to me but is not available for comments. His note has a lot of data but is inconclusive, as best. On the other hand very many economists have supported it. So it is better to go into each issue on its merit.

An estimate of black money -

Black Economy and Black Money are different. The second is the part of the first. The total value of 500 and 1000 rupee notes is 14 lakh crore of rupees .There is no estimate of black economy which consists of land, real estate, jewellery and cash. Only the cash portion is black money. If there is any illegal activity (like under invoicing or building with under declared value of materials) going on, generating black money will be the end product. There is black economy estimate given by chief economic adviser of SBI which is 45 Lakh Crores. He has estimated on the basis of SBI Research and RBI. Dr. Arun Kumar who has written a book about black money has written in his note that it is double the amount but he has not given any calculation. He has said that the black money will be a small percentage of the black economy. If you take it as 10 lakh crores then it is comparable to what Chief Economic Adviser has said that the unaccounted black money is one fifth of 45 lakh crores. That comes to 9 lakh crores. So both the estimates of SBI and Arun Kumar agree practically to 9 to 10 lakh crores. So we can reasonably proceed on an amount of 10 lakh crores as black money. Total amount of money in circulation in 500 and 1000 rupees notes is 14 lakh crores. It has been estimated by Chief Economic Advisor of SBI that 4.5 lakh crore rupees will not come back to the system. There is another calculation discussed below.

How much black money will be useless paper-Really how much money can be retrieved?

Can clever people get round it? Manish Sabharwal has written that in Mumbai betting pool says that between 20% and 40% of the black money in circulation will not be deposited by December. Two crore lakh rupees will be become useless paper. The argument of Arun Kumar and Prbhat Patnaik that clever people will get around their demonetization is not correct with this calculation. Earlier in 1978 there was no limit but this time there is a limit of two and half lakh above which government will ask how they got the money, So people will be afraid to enter into any risk . Arun Kumar`s idea that Jan Dhana Yojana accounts will be used is only a pessimistic imagination. So this time the black money that will become useless will be much more than expected or what was in 1978. Already several bags of big denomination money have been found abandoned in Kolkata near Tolly Golf Course and in Bangalore near Banaswadi fire brigade.

Fake Money

An estimated amount of 400 crores of fake money will be eliminated. Manish Sabharwal, Chairman Teamlease Services has said that to people born in Kashmir such as him, it is obvious that much of valley terrorism is fuelled by money not printed in India.

Black economy will get a jolt -

Middle class beneficiary-I checked up from property agents and house owners that property price has fallen and the black money equivalent has vanished. One property owner near my house put up board for rent changing his mind for sale due the latest action of Modi. Now middle class people will find it easier to buy property. Mispricing of real estate had earlier stood on the way to entrepreneurship, global competitiveness and job creation.

Bold policy -

It is a bold policy because it will ruin the black money held by not only all other political parties but also those held by BJP itself. There is a vague hint given by some writers that BJP already looked after its stock of black money. The only estimate that somebody has given is that 3Crores have been deposited by BJP functionaries in advance. As if 3 crores is the only amount that a party has!

Demonetisation: Impact on stock markets

Flow vs stock -

True, it will destroy the stock and not the flow but it will take long time to create the flow given that the government is also taking steps to stop the flow by GST and several other schemes simultaneously.

Hawala -

Arun Kumar says hawala will increase. It will not. For hawala operators will not accept demonetised notes.

Gold -

Assumption that people will buy more gold is wrong as the gold or ornament merchants will not accept old 500 and 1000 notes.

Recession -

Some economic activity which depended on payment by black money may slowdown but soon they will resume momentum with white money.

Fall in GDP-

That will not take place. At the macro-economic level whatever is the level of black money coming to banks by December end and into the RBI by March end, and in consideration of what has not come and what cash was issued earlier, RBI will arrive at a calculation of change in liabilities and quantify mismatched assets and liabilities in its balance sheet. It will then return some government bonds it holds thus enabling government to enable spending and in turn restoring the GDP to normal.

Rs 65,250 crore already unearthed -

Under the Income declaration scheme - One famous economist has said that it could be also the effect of ongoing effort of income tax officers. Nevertheless even if that is true, the unearthing of this much of black money is significant.

Growth- Developed economies have less black money -

Developed economies have less black money. An international chart has been prepared by Arun Kumar in his book. This chart is a collection of several studies by international experts. It shows that highly developed countries have less black money than less developed countries. So it follows that less black money is a step towards a more sustainable development.

Ease of doing business - will improve with less black money.

Interest rate for lending-
Will go down with so much of cash coming to the banking system. H.V. Kamath Chairman of Brics Bank has also confirmed this likely effect.

Lack of banking preparedness -
Those who complain about less banking preparedness should know that such a secret policy could not be introduced with previous preparation. I have handled three of sudden policy changes in my official life. First, on 6.6.66 devaluation of currency was done. We in the Custom Houses assembled and decided to visit where ever clearance could take place in the night like from oil installations. Also all documents were revised next morning. Second, during Emergency suddenly announcement was made that Customs could preventively detain smugglers under amended MISA. So we worked night and day and prepared dossiers and detained a large number of top and other smugglers. Thirdly, when in 1978 Sikkim became part of India, we immediately moved our customs and other administrative machinery there. Again in 1980 this happened for central excise. For secret introduction of policy, there cannot be any advance preparation.

Multiple-rated GST- will it create black money?
Not significantly. Very little! It will obstruct ease of doing business and increase corruption but black money generation will not be substantial.

Black mentality -
The whole black mentality will suffer a jolt. Nobody believes now that you could have a all- white transaction. Really it was still possible. Several people have done it but they are the exceptional persons. People often too easily succumb to temptations and downright greed and then blame the system. Now with this move to severely damage the kingdom of black money, more people will look for all- white deal.

Conclusion -
It is a fundamental reform in India. After decades of rhetoric, some real action has been taken. Demonetisation along with all other policies such as Jan Dhan Yojana, Aadhar, mobile banking, Bharat Bill Payment, GST, the Income Declaration Scheme to declare black money, and also next scheme to act against Benami property will ensure a real impact on black money.

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 / 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!***

A Security Professional's Chronicle

Capt G Rajkumar

Capt G Raj Kumar is ICISSM Councillor for Andhra Pradesh and has total 29 years' industry experience out of which he served 14 years in the Armed Forces. He has unique distinction of serving in Indian Air force as well as Indian Army. While in Army he has been involved in Counter Insurgency Operations. He holds MBA (HRD) and presently pursuing Ph. D in Personnel Management. A keen sports enthusiast, he represents AP Badminton Team. He also plays in badminton tournaments by Petroleum Sports Control Board. He has represented India Veterans' Category in a world Championship tournament. He can be contacted at: grajkumar@gail.co.in or captgrajkumar@gmail.com

Security professional challenges within are of utmost importance than that of external. It has been evident that lack of professionalism is haunting the security profession, of late. As the threats have seemingly complex and are faceless. Adding fuel to the fire, the rapid growth of technology is aiding the anti-socials / thieves to have edge over us. Crimes of faceless, boundary less, virtual, remote-controlled, hi-tech and criminal cosmopolitanism have further burdened our shoulders. To my insight, in this environment the only way to survive is to follow the way as enumerated by the great Sun Tzu -

> "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also

suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle".

Thus it is warranting us to be more tech-savvy and forethoughtful. As everyone in this profession would agree with me that unlike other departments or professions, we do not have scope of pass percentage or % of target achieved. We have only two parameters i.e., either we pass or fail. In other words, we may conclude saying that if we provide an incident free period, we may call it 100% success.

In recent times, more and more companies are tilting towards technology and acquiring various technical gadgets in a big way. Everyone talks about CCTV, Baggage Scanners of various types, Bollards, Access Control Systems, etc.,

It is definitely a good sign, but then, there are certain aspects which need to be deliberated upon for a better output and ROI (return on Investment). Technology abundance, variety of gadgets and mushrooming business firms selling them has created a type of confusion in the minds of us i.e. end-users / security professionals. This is an inherent challenge we are facing now. In this situation either we depend on some technical departments or copy the specifications from someone who have already done some homework on this. The other intriguing aspect of present day is that someone has installed a high-tech security gadget, and, we decide to install similar or preferably a better or higher technology gadget in our organization. This results into a situation when most of the advanced features and applications remain unused or undesired. Someone has said that, "If we think that technology is going to solve all our problems then we either do not understand our problems or we do not understand the technology!"

I am of firm opinion that 'Science is good servant, but a bad master'! Let us use it optimally. Let us not totally depend on technology. Technology after all is as good as men behind the machine! Emphasis on human resources improvement / development should be given priority at par with technology. Whereby, the technology would complement the manpower to get maximum benefit /outcome. In this process there are certain points which I would like bring out here:

1. Man behind the machine has equal or more importance than the gadget. Hence, they are to be given due diligence in selecting.

2. Train and re-train the available human resources at our disposal for augmentation of existing security set-up.

3. Acquire compatible, suitable and relevant security gadgets rather than going for sake of it or following others or going for higher technology.

4. Lack of customer oriented and suiting software for various technical gadgets available in the market and complex & ever changing nature of threats compelling us to declare gadgets as 'obsolete' in very short period.

5. Adding to this is rapid technological advancement and substandard equipment floating in the markets. The price range of such equipment is mind boggling. You would get a CCTV camera with almost similar specifications for a very surprising price range. One can use a Rs.350 camera brought from Gaffar Market, New Delhi or use a reputed brand camera

costing almost Rs.7,000/-, the quality of the footage has no drastic difference. This is an example to state that the range is wider.

6. There is a short-fall or slackness in developing a road map for implementing a well-planned enterprise level integrated security systems set-up. Most of the organizations go for a piece-meal procurement and installation of few security gadgets. We as professionals can chalk out a plan for systematized implementation of 'Enterprise Security Solution'. Wherein any gadget procured should fall in the already chalked out plan only. This way one can, over a period of time, implement the road map and integrate the gadgets on one platform. This we may call it enterprise security umbrella. This is good for bigger organizations as well as small organizations or residential houses/apartment.

7. We, Security professionals, should develop a habit of making notes of events, incidents, accidents and other activities nearby or concerning.

8. By generating lot of data, we should also be able to analyse the same and put to use for benefit our profession. As it is rightly said that "Noticing small changes early helps you adapt to the bigger changes that are to come".

9. Many organizations do not take in to account the security aspect at blue print stage whereby end-up in spending a lot in modifying the already built structures / perimeters. In many western countries, and, in fact in many of our country's top business houses, the Security Department's input is considered at blue print stage itself. Here it is the security professional's task in proving his / her competence by implementing CPTED (Crime Prevention through Environmental Design). This helps the management decisions, since it gives due importance and value for environment as well as aesthetics.

10. Finally come what may be, the vital element of Industrial Security or Residential Security or any form of security is 'right manpower' for it to be effective and efficient.

11. The established wisdom of criminology is "Crime follows Opportunity", hence our prime motto should be "Opportunity Reduction"

12. To my knowledge, common-sense, forethought, planning, timely implementation, system monitoring including feedback, review and redesigning are the vital elements of security profession. With this emerges a thumb rule of Security 'ASC':

A	Assume Nothing
S	Suspect Anything
C	Check Everything

Stay secured! Happy New Year!!

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

Suggestions & feedback may be sent to us on e-mail: onlineicissm@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!