International Council of Industrial Security & Safety Management

Monthly Newsletter
April 2017

Exploring open source software opportunities.

What does the Security End-user seek from a System Integrator?

Open system standards have basis requirements such as that they must be defined fully, so that vendors can work within the same framework and be stable over a reasonable length of time, so that the vendors have fixed targets to aim at. In context of security systems, Open System is an open source operating system, typically composed of coordinated modular components from a number of sources and not reliant upon any proprietary elements. Characteristics of open systems include the exposure of the source code, which is available for understanding and possible modification and improvement; portability, which allows the system to be used in a variety of environments, and interoperability, which allows the system to function with other systems.

To remain competitive and to retain the edge, many OEM invest heavily in R&D and have very good 'deliverables' which become their USP. To think that they will have 'open system' is not practical. Where are the open systems which use widely supported and consensus-based standards for its key interfaces in security management technologies? In true sense, I mean!

Why someone with hard work and expenditure develop a technology and bring it in public domain for common use? When such technologies out-lives patent conditions and come in public domain, other technologies are brought-in through product development and R&D and thus good OEM will always maintain the edge and retain the market share. Market leaders will thus be those who have latest technology and end-users will prefer them even paying higher price since this affords them the advantages which Open Systems do not!

With very best regards

this issue ...

Open System - How far?

The Open System is chimera, an illusion forwarded by generalist system integrators, though aspired by the Security System Operators and security professionals! There are presently really no 'open systems' and those sold and bought as such prove to be otherwise later on when technology up-gradation, 'stand-alone' systems' integration or modular expansion is needed! At that time technology providers indicate those conditions which are in fine prints which no one reads!

OEM support has contractual time limitations. For seamless software and hardware integration with other systems, there is need to have uninterrupted dialogue between them. SDK is one issue that needs to be resolved with-out which there cannot be any open system. Many system integrators or solution providers fail on this account. Software licence too has number and time limitations.

Embracing Global Change and Paradigm Shift

Being an Intelligent and Secure Organization for the Future

DC Nath, IPS (Retd.)

The author is Former Special Director, Intelligence Bureau, Government of India. Author of various books on homeland security, intelligence and industrial security, he is globally acclaimed domain expert.

He is Chief Patron of International Council of Industrial Security & Safety Management

It is necessary to know and appreciate what is the threat or challenge before us today – both as human beings per se and as security professionals in particular. The concept of a conventional war between two countries is now considered a passé. So has observed John Horgan, Director of the Centre for Science Writings at Stevens Institute of Technology, in a brilliant write-up, "The End of The Age of War", appearing in the Newsweek Special Edition – Issues 2010: "War seems to be a cultural phenomenon, which culture is now helping us eradicate. Some scholars even cautiously speculate that the era of traditional war – fought by two uniformed, state-sponsored armies – might be drawing to a close." "War could be on the verge of ceasing to exist as a substantial phenomenon," said John Mueller, a political scientist at Ohio State University.

The real threat today comprises continued acts of violence, state-sponsored or otherwise in different parts of the world, more popularly described as acts of terrorism. Transnational terrorism is the real threat today before all of us. Notwithstanding the fact that so many advanced countries spend fortunes in military spending, "The past year saw increasing threats to security, stability, and peace in nearly every corner of the globe," the Stockholm International Peace Research Institute recently warned. Many nations and countries are now in fact faced with the phenomenon what can be best described as 'globalization of violence', be that genuine liberation movements or motivated groups practicing terrorism covered by a very thin veil of political pretensions.

"It would be a gross error to treat the terrorism facing India — including the terrible recent atrocities - as simply a problem for New Delhi alone. In a very real sense, the outage in Bombay and elsewhere was fundamentally a species of global terrorism not merely because the assailants happened to believe in an obscurantist brand of Islam but, more importantly, because killing Indians turned out to be simply interchangeable with killing citizens of some fifteen different nationalities for no apparent reasons whatsoever."

- Mr. Ashley J Tellis, Senior Associate, Carnegie Endowment of International Peace. (Indian Express – January 29, 2009)

There is thus an imperative need to appreciate the precise nature of the threat which marks the major paradigm shift in the history and growth of terrorism. One has to acknowledge this unambiguously. It is now global or universal jihad, which is a threat to all free world countries and it is a war that can be won only if we acknowledge that it is a war against humanity. Unless this is appreciated in the correct manner, the entire approach to handle terrorist threat could be faulted. Perhaps it is this lack of political will, to call a spade a spade is causing such enormous problem today in Pakistan which is at the receiving end from the Taliban. Much of the problem in India also could be attributed to the lack of admission of reality and feeble attempts at taking cover in the name of functioning in a democratic form of government. LeT is now the virtual substitute for Al -Qaeda with Yemen as the latest base station.

Globalization of Violence

Coming down to more specifics! Even though unanimity of opinion is still lacking over the definition of terrorism, common refrain in all understanding or analyses of terrorism, veers round to what is described as jihad or jihadi terrorism. Jihad is a war or struggle against unbelievers and is waged by a number of groups owing allegiance to Islam.

This was proved most emphatically in the 26/11 massacre at Mumbai (India). Reputed international commentators have described it as the seminal event in the history of international terrorism and particularly in the history of global jihad. The following will further illustrate it:

"The attacks on Mumbai are part of a global problem."

"Ignoring the ideological Islamic violence denies the existing reality of the Mumbai events."

"To pretend that such deaths were caused by old complaints in Kashmir is to ignore the real threat and thus to endanger humanity."

- Stephen Schwartz, Executive Director, Irfan Al -Alawi - International Director, The Centre for Islamic Pluralism - The Spectator.

(The Asian Age - December 6, 2008)

Embracing Global Change and Paradigm Shift

Being an Intelligent and Secure Organization for the Future

The United States of America and UK have also been warned of 26/11-like acts of terror. The problem there has become more complex because such threats are no longer posed by non-state actors from outside but are also from home-gown terrorists, a fast emerging phenomenon. Female participation in jihad adds a further and new dimension. "A significant development in women participation in the global jihad has been the dissemination of radical ideologies on-line", writes Mia Bloom in a draft of her forthcoming book, "Bombshell: Women and Terror" (*Time, February 1, 2010)*.

Another major paradigm shift is in the technique of perpetrating acts of terrorism. Apart from perfecting the art of suicidal Fedayeen attacks, there has been tremendous sophistication in the methodology being adopted by the terrorists. There has also been substantial qualitative improvement in the profile of the terrorists involved, as revealed in the analysis of the character and antecedents of those involved in 9/11 or the series of terror attacks in India, involving educated and technically equipped youth representing the Student Islamic Movement of India (SIMI). Talking about the 9/11 group, Steve Coll, a Pulitzer Prize Winner, has said in a recent interview, "those guys were not nuclear physicists but they were well-educated, smart, determined, careful and willing to learn." He further added that while AL Qaeda had thus been able to put together really talented people, Lashkar's style of talent is more worrying. Some of the proselytizing networks have been able to recruit and radicalize scientists, doctors and other such talented people from here and there, as seen in 26/11.

They can wreak a lot of havoc. (*Steve Coll, Pulitzer Prize Winner, The Indian Express, New Delhi, January 26, 2010*).

There has been a distinct trend in exploiting knowledge gathered from information technology, as seen in a spurt in the number of websites, which were earlier hosted for raising funds but now are being used for offering training and dissemination of ideology and other technical know-how. Steganography, that is, sending coded messages through pornographic pictures, was adopted in the December 13-attack on the Indian Parliament. Threat of cyber attack has indeed pushed the United States to plan for independent Cyber Command. This is nothing but the real case of power of information technology, another paradigm shift.

So, what do we do to face the situation? India, even after more than a year after 26/11, is still described as a "sitting duck". The Union Home Minister, Government of India, has candidly said 'India remains vulnerable'. The Government of India is engaged in working out a new security architecture and is also concerned with developing intelligence for the world of tomorrow, as its Vice President has said the other day. Many other countries will also be undertaking such exercises. All these are, however, preparations for facing the emergency or critical situation once an act of terror has taken place. That is, the authorities would now be able to face the situation in a more organized and effective manner after an act has taken place or has been launched. But, what about creating the situation or ambience which will not allow the terror philosophy to grow or gain roots, and if it grows, to nip it in the bud without overreacting to the same? This is specially relevant to functioning democracies. India is supposed to be a model for this. A lot of other democracies have dealt with the problem of persistent terrorism without surrendering their values. So has said Steve Coll "democracies go through stages of learning about how to deal with the persistence of terrorism."

A new and vital paradigm shift in approach to tackle terrorism should, therefore, lie in spending more time and thought on preventing terrorism to grow or take roots and tackle it with a long term perspective and with societal participation. As it is said, security is business of all, for all and by all.

That is why it is recommended that the corporate world should try to educate its employees in the matter of security concerns by way of encapsulating security doctrines in their corporate social responsibility (CSR) policy. Employees will then help build up the national resilience against all forms of security threats including terrorism.

The paradigm shift in approach to tackling terrorism problem today really lies in the concept of public-private partnership. Countering terrorism is not just a job for the security and intelligence services.

Embracing Global Change and Paradigm Shift

Being an Intelligent and Secure Organization for the Future

Yes, there is indeed an imperative need for improving infrastructure and intelligence gathering. The difference between victory and defeat has been rightly described as availability of good intelligence or the absence of it. Such good intelligence could really come up and be built through the module of perfect public-private partnership. Intelligence is the backbone of all political stability which can in other words be put as the by-product of good internal security mechanism. Modules of private-public partnership have been very successfully worked out in the UK through Project Argus and Project Griffin.

Project Argus relates to "resilience planning". "Responding to a growing concern amongst business for a need to be prepared in the face of terrorism and to bring vast public and private sector expertise together, London First has established a growing Business Security and Resilience Network since 9/11. The Network brings employers, police and government emergency planners together to share expertise and encourage co-ordination of business continuity activities across sectors. Members are also linked up to London-wide fast-time incident alerts as well just launching a quarterly political and fraud intelligence briefing service."

Project Griffin deals with how police can take advantage of the bulk of private security force available in the country. It is a community outreach program institutionalizing cooperation between the police and private security agencies under three basic formats, within the overall scheme of Counterterrorism measures known as Preventing Extremism Together (PET). These modules are being implemented in many other countries.

It is, in this context, incumbent on the corporate world to undertake security audit and then undertake risk management study, not only to get the Return on Investment (RoI) but also to ensure what is popularly known as business continuity planning. Diligent business continuity planning leads to saving of expenditure. That will also lead to real convergence of both business interests and security interests. If a forward-looking business entity spends money on modernization of its management technology and on methods of improving production technology, why cannot it also think in the present-day security ambience of spending money on modernization of security technology, investment of some money on research relating to security management? Investment in security will never go waste. Unfortunately, management often forgets that security is amongst its vital tools to increase operational or functional efficiency and thus to increasing production under secure conditions. This paradigm shift is also essentially called for.

The concept of 'good citizen'

In order to build up an intelligent and secure organization for the future, it is not enough to revitalize the internal security mechanism or even reforming the entire criminal justice system in a country.

Equally, if not more, important will be to help develop the spirit of national resilience through a carefully structured public-private partnership, educating the people at large and thus leading to the creation of what we would like to call "good citizens."

The concept of 'good citizen' has to take root in the manner envisaged in Article 51-A of the Constitution of India, spelling out the fundamental duties of the people.

All of us need to embrace and imbibe that culture and the spirit in toto and that is the mantra for success and survival.

common_heaven@yahoo.co.in

Cyber Attacks guiding Large Enterprises as well as SMEs to integrate Web Application Firewall (WAF) with DDoS mitigation to protect ROI & SLA: Col Prabir Sen, Veteran

Cyber-attacks are growing in its scope and scale both, with ever emerging and more complex security threats. Recent market trends suggest potentially targeted strategic and business entities migrating towards WAF integration with other solutions, such as advanced endpoint security and distributed denial of service (DDoS) protection.

"HaltDos", an Indian Institute of Technology, Delhi incubated innovative Technology Start-up has launched Cost Effective – DDoS mitigation solution with Web Application Firewall (WAF), a fully managed solution that uses state of the art anomaly detection techniques to block Application Layer Attacks with zero false positives. It protects websites and SaaS based Applications, from common and zero-day web exploits that affect application availability, compromise security or consumes application server resources. It also periodically goes and audits your website & web based applications, to provide comprehensive security for your website.

"HaltDos" SaaS based Web Application Firewall solution provides the fine-grained configuration and application server level monitoring that provides full spectrum visibility with no single point of failure.

HaltDos- WAF Features include:

· OWASP Top 10 Threat protection

· Bot Attack Protection

· IP Reputation

· Geo IP Throttling

· Built-in Rules

· Custom Rules for Business Logic

· Clickjack Script Injection

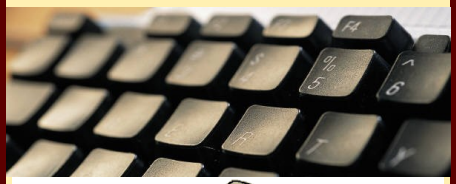
· HTTP Misbehavior Protection

· Periodic Security Audit

· Instance level monitoring and

· Actionable Reports

· "HaltDos" also offers free trials, training and handholding to end users prospects.



Software Piracy

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business Software Alliance (BSA), about 36% of all software in current use is stolen.

Apart from employing Corporate Risk Managers, IT Managers, and also making use of security defence solutions (firewalls) and protection systems (IDPS), it has become necessary for companies to conduct training for everybody as part of the security strategy to reduce exposure to data integrity attacks and other threats. As breaches become more common, to take security awareness on board in an organization can reduce risks. Educating users can help lessen the chance to become victim of an intrusion attempt that targets one of the weakest links in the cybersecurity chain: end users themselves.

The importance of security awareness training

Nowadays, security awareness training (SAT) is a top priority for organizations of all sizes. The Management and the Employees can understand security governance issues and control solutions as well as recognize concerns, understand their relevance and respond accordingly. Many companies invest heavily in security education programs for employees to learn how to protect their moveable properties, laptops, computer and personal information and how to be aware of many criminals that scour the office premises and the Web in search of targets and vulnerabilities.

The Importance of Security Awareness Training

Security can't be guaranteed. As Clint Eastwood once said, "If you want a guarantee, buy a toaster."

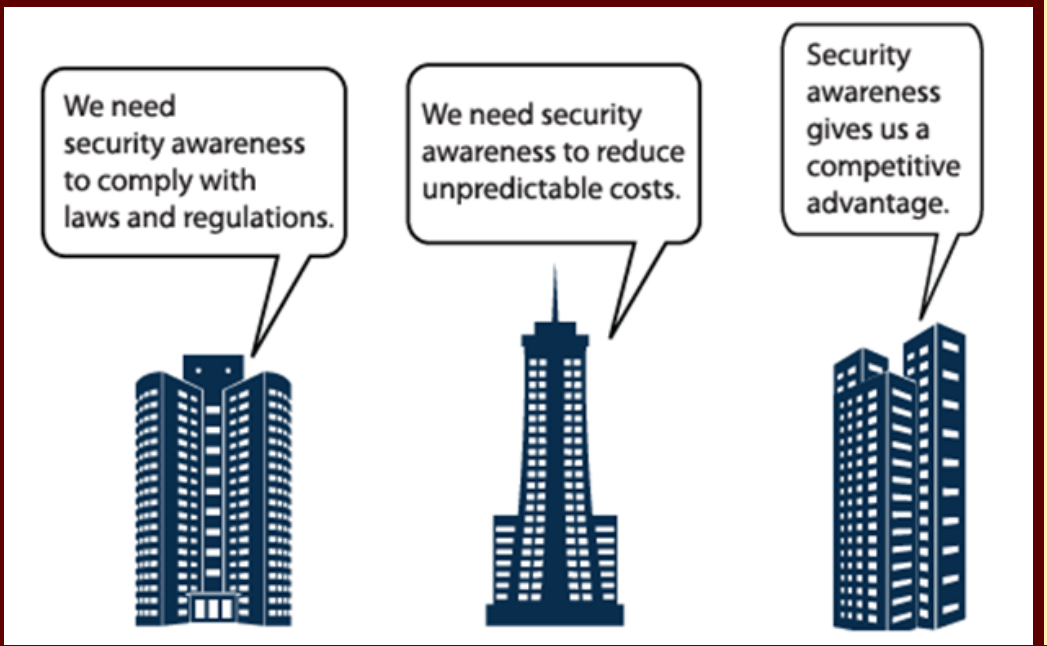
The British have a marvelous word - "whining" - which refers to the practice of complaining without doing anything about it. As in, "Everybody whines about the weather, but nobody does anything about it." We may not all call it by this name, but security practitioners in every country love to "whine," because it's so much easier to whine about a problem than try to fix it.

Over the last few years, the volume of industrial security whining has been deafening, thanks in part to the legions of newbies whose expectations don't square with reality. Even after the high-tech meltdown, the vendor space is filled with goofy products developed by technologists who don't know the difference between need and demand. The industrial security professionals keep cribbing that their management is indifferent to their needs whereas the vulnerabilities keep mounting! What they do not appreciate that it takes only marginal efforts in providing awareness training to their employees.

One of the best ways to make sure company employees will not make costly errors in regard to security is to institute company - wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness websites, helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.

One of the greatest threats to security could actually come from within your company or organization. Insiders have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee!

Educating employees about security is a vital part of your defence against criminals and unethical competitors. Yet security training and education is often neglected, sometimes at great cost. A breach of your company's security can be hugely expensive, dwarfing the cost of the training that could have prevented it. To learn the role of education in security and discover ways to implementing training without breaking the budget remains one big challenge to the management and security in-charges!



Security awareness can be the most cost-effective security measure!

- Ira Winkler

Professional Development

Dear Friends,

We once again bring to you the best global opportunity to upgrade you professional knowledge and learn from the world's best!

We are proud to announce partnership of ICISSM with PCS Training Consultant in organizing 3rd Annual Global Energy Security Conference at Cebu, Philippines.

The esteemed members of ICISSM will get 20% discount in delegation fees and they will have learning opportunities from the world's leading security professionals and strategists. The conference also offers great networking opportunity to the professionals.

Upcoming Events

For more details, please contact -

Policarpia C. Secretaria Jra.
Conference Director
PCS Training Consultant
Lipata, Minglanilla
Cebu, Philippines, 6046
T: 0063-260-05-57
M: 0063-9064116749
IP: 001-777-8874-421
E: polly.secretaria@pcstconsultant.com
W: www.pcstconsultant.com

Upcoming Events

Professional Development

Tech Times
ISSUE 00 MONTH YEAR

Pinkerton CRM India, International Council For Security & Safety Management (ICISS) and FICCI have launched India Risk Survey 2017.

The esteemed members of ICISS and the readers of its newsletters will be happy to note that ICISS is helping and supporting this survey. The survey is an attempt to recognize possible risk factors while operating in India. The end result of this survey will also be shared with Indian government that will be eventually referred to formulate regulations, critical policy enhancements and strategic decision for commercial organizations. The previous survey results were effectively used by many organizations world over to learn about risk dynamics in India. We value a professional like our readers of the newsletter and members of ICISS and are very keen to get your expert comments through the survey. You can fill the survey by clicking this link:

http://irs.pinkertonindia.com.

International Council of Industrial Security & Safety Management
111 – GAIL Society, Sector Pi (I&II), Near Eldeco Riviera, Greater Noida, Gautam Buddh Nagar, UP
Mails: onlineicissm@gmail.com
Blog: http://captsbtyagi.blogspot.com
Web-site: http://onlineicissm.wixsite.com/iciss

Forthcoming Events

Key Highlights: Launch of "India Risk Survey - 2017" Report.

PARTNERS

Knowledge Partner:

PINKERTON®

Supported by:

ICISS

Media Partners:

SecurityLink India

IMR

To participate in the survey, click on the link below:
http://irs.pinkertonindia.com/

BLOCK YOUR DATE

Contact Us

Mr. Sumeet Gupta
Director
Federation of Indian Chambers of Commerce & Industry (FICCI)
E: sumeet.gupta@ficci.com
T: +91-11-2373 8760-70 (Extn. 515)
F: +91-11-23765333

Ms. Bhawana Sharma
Assistant Director
Federation of Indian Chambers of Commerce & Industry (FICCI)
E: bhawana.sharma@ficci.com
T: +91 - 11 - 23738760-70(Ext: 443)
F: +91-11-23765333