AP Dynamics

The official Newsletter of ASIS International in Asia-Pacific

February 2014, No. 7

Quick Links

Register Now

Sponsor/Exhibit

In This Issue

Welcome to the 7th edition of ASIS International's *AP Dynamics*, the monthly newsletter for ASIS members in the Asia-Pacific region covering ASIS news, chapter news, and important Asia-Pacific headlines.

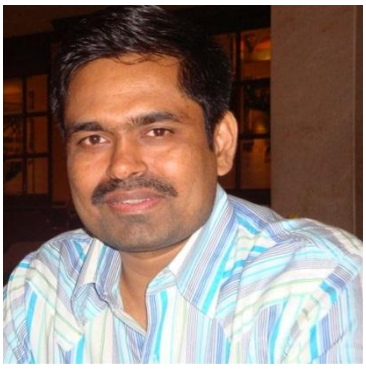
The ASIS Asia-Pacific Bureau invites members to submit updates or articles to share with fellow members in the Asia-Pacific region. Please note that ASIS board-certified professionals are entitled to up to 9 CPE credits per article.

The submission deadline for the next issue is March 5.

In this issue: Ratnakar Bade, CPP, explains the importance of loss prevention programs in high-value manufacturing. Small supply-chains partners are increasingly being targeted by advanced persistent attacks. The first Asia-Pacific cyberintelligence centre has opened in Singapore. Critical sectors in India have received cyber-attack protection. Increasing mobile traffic volume in the Asia-Pacific region through 2018 is expected to increase the CSOs' security burden.

Please add regionalnewsletters@asisonline.org to your personal address book or safe sender list to ensure correct delivery of your monthly newsletter.

Loss Prevention Program in High Value Manufacturing



By Ratnakar Bade, CPP

Join Us on Facebook

ASIS 60th Annual Seminar and Exhibits, Atlanta, Georgia, USA, 29 September-2 October, 2014

Like us on Facebook

Join Us on LinkedIn

Join the ASIS International Group

Join the ASIS Asia-Pacific Network

President's Perspective

ASIS International's 2014 president, Richard Widup, CPP, shares his unique

Challenges and Objectives
In high-value manufacturing, costly components are susceptible to mishandling, damages, discrepancies, pilferage, and possible thefts. They can be easily carried unnoticed, as many defy metal detectors. As production targets are time-sensitive and quality-driven, component shortages at assembly lines may result in huge losses. To proactively mitigate these risks, security teams need to implement process controls on the shop floor that go beyond premises and personnel security. The challenge is to initiate an effective security structure while maintaining prudent employee relations. The imperative is to set up process-driven and consistent loss prevention program.

Focus areas

1. Governing structure
2. Proactive risk management
3. Security systems
4. Warehouse security
5. Supply chain/logistics security
6. Effective guard force
7. Continual improvement
8. Standardization and benchmarking
9. Employee awareness
10. Collaboration

Governing Structure
A security steering group (SSG) should be formed. The SSG should be composed of a managing director as chairperson and a security manager as convener with responsibility to run the proceedings. Other members are managers from production, HR, facilities, planning and logistics, finance, and legal. Business risks and challenges, mitigation plans, and security projects are reviewed by the SSG, where quick decisions are made. A security implementation team (SIT) should be formed from within the SSG. The team's cooperation in implementing security controls and other decisions made by the SSG is crucial.

Proactive Risk Management
Security controls are based on risk assessments. Annual or biannual risk reports should be presented to the SSG for approval of the mitigation plans. Risk assessments should include all processes, dependencies, systems, and resources.

Continual Improvement
It is necessary to sustain the procedural maturity that is achieved through systemic controls, as well as to further improve it, by incorporating lessons learned, the outcomes of testing and exercises, stock loss trends, and stakeholder feedback. Plan-Do-Check-Act is one effective methodology that can be used.

Employee Awareness
Employees need to know risks to operations, people, and property, and to understand certain controls -- some of which may be deemed cumbersome. Therefore, the security team needs to be innovative in ensuring effective awareness to sensitize employees on risks, expected behaviors, and compliance.

insights on a range of membership and industry issues in his President's Perspective column. Read the latest here.

Did you like this issue?

The Asia-Pacific Bureau of ASIS strives to present content of the highest quality to ASIS International members.

Please contact the editor to contribute feedback and make article submissions.

ASIS Asia-Pacific Bureau

Queries on ASIS International Asia-Pacific events, membership, benefits, resources, or certification, can be addressed to:

ASIS Asia-Pacific Bureau

300 Avenue de Tervueren,
1150 Brussels, Belgium

Tel: +32 2 645 26 74
Fax:+32 2 645 26 71
asiapacific@asisonline.org
www.asisonline.org

Asia-Pacific Links

Please visit our Asia-Pacific chapters' Websites at the following links:
www.asisaustralia.org.au

www.asis.org.hk

www.asisindonesia.or.id

www.asis-japan.org

www.asisseoul.or.kr

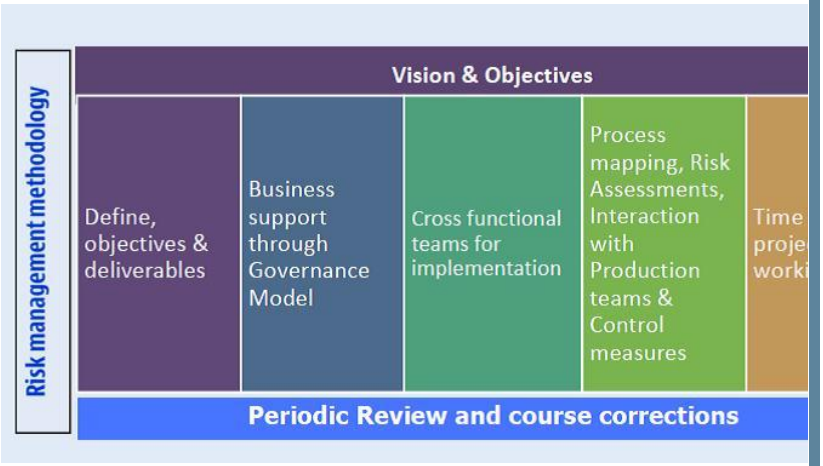
www.asis.org.nz

www.asis.org.ph

www.asis-singapore.org.sg

Collaboration
Structured collaboration with stakeholders is needed to plug loopholes and ensure protection of assets and information. Risk Management methodology requires buy-in to get corrective action plans (CAP) implemented, as risks that emanate during production processes must be mitigated by production teams. Continual improvement to reach a financially optimum security solution needs mutual information sharing and continuous feedback.

Management System Approach
A structured approach requires a management mandate, time-bound objectives, and teams with roles and responsibilities. The security manager should bring progress reports to management for its review and input. An open, transparent, and optimally visible program will reinforce the strategic importance of corporate security.



Conclusion
A security program needs a management mandate, employee support, and visibility. Its success depends on structured, process-driven and consistent programs implemented through prudent techniques and a competent guard force. The security manager has to be a diligent and innovative leader and a multitasking manager who can effectively communicate through diverse echelons. Corporate security can be established as an extremely disciplined, business enabler and an employee-friendly function with a professional, impartial, and compassionate approach.

Ratnakar Bade, CPP, has been in security profession nearly 22 years. A former infantry officer, he has worked in diversified sectors such as defense, financial,and telecommunications, and has sizeable experience in manufacturing and research and development. He has special interest in management systems and is a lead auditor for business continuity and occupational health and safety. Presently, he works for Nokia, leading the security services team for the IMEA Region. He is also an active volunteer for the ASIS International Mumbai Chapter.

www.asis-thailand.org

Not Yet a member?

Ten reasons that you benefit from becoming an ASIS International member:
- Unrivalled networking opportunities with more than 38,000 of your industry peers.
- Up-to-date information, including industry best practices, new technologies, and emerging trends.
- A complimentary subscription to *Security Management* magazine, the leading security industry publication.
- Opportunities to build a professional reputation and credentials.
- Tailored professional development programs to fit your specific career goals.
- Advocacy of the security industry to the government and business communities.
- Board-certified, professional designations.
- Members-only access to new career opportunities in security management.
- Access to more than 300 peer-reviewed, security-related publications.
- Discounts on program and Seminar and Exhibits registration, merchandise, and certification programs.

More Information...

Select ASIS International-Published Titles Now Available for Purchase for Amazon Kindle

- *POA: Physical Security; Applications; Information Security; and Investigation*

ASIS International News

ASIS PCB President: Blurring Lines Between Public, Private Sectors

ASIS Professional Certification Board (PCB) President Owen J. Monaghan says that one of his goals for his current term, which will run through the end of the year, is to increase the number of security professionals who are ASIS-certified. Monaghan, who is also the assistant police chief of the New York City Police Department and is the first active-duty police officer to serve as president of the PCB, says one reason why he wants to promote ASIS certification is because he has benefited from having a Certified Protection Professional (CPP) designation himself. Monaghan says that having this designation gives the private sector partners he works with in securing infrastructure, events, and venues the assurance that he is knowledgeable about security issues. Certification can benefit other security professionals as well, Monaghan says, because PCB's certs are kept up-to-date with changing skill sets and because they are relevant for any industry. In addition, security professionals who are certified have demonstrated that they have a "passion for knowledge" that is valuable in the workforce today, Monaghan says.

Source: Security Director News

Please click here for more.

2014 ASIS Membership Renewal

Renew Now

It's time to renew your ASIS International membership for 2014. Don't let your member benefits become interrupted.

To renew, visit the "My ASIS" section of the ASIS Web site; after signing in, select the **"My Transactions"** tab to see the dues renewal invoice. Your membership can be identified by the **"Member Type"** populated in the far right column. Please select the invoice and choose **"Add to Cart."**

For assistance, contact ASIS Member Services via e-mail at asis@asisonline.org, or by phone at +1.703.519.6200, from 9 a.m. to 5 p.m. U.S. Eastern Time, Monday through Friday.

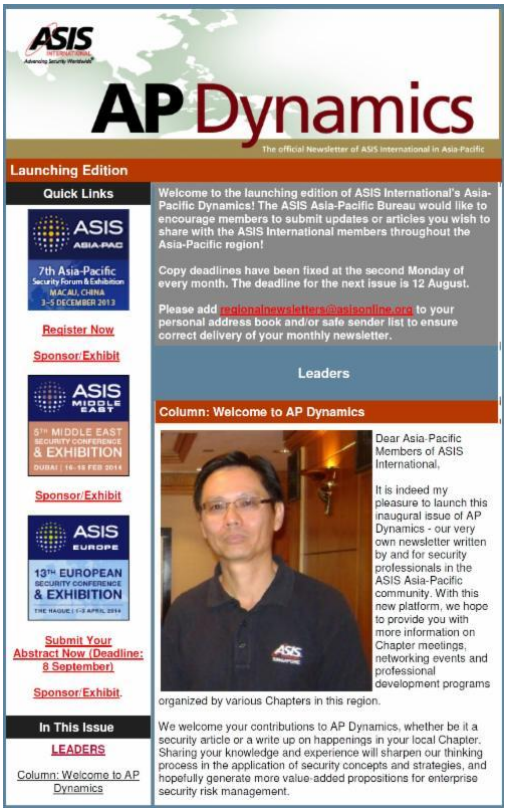
Stay connected in 2014. Renew your membership today

- *POA: Security Management; Legal Issues; Security Officer Operations; and Crisis Management*
- *Active Shooter: A Handbook on Prevention*
- *Career Opportunities in Security*
- *Casino Surveillance and Security*
- *Crime Prevention for Houses of Worship*
- *Detecting Forgery in Fraud Investigations*
- *ASIS Disaster Preparation Guide*
- *Emergency Planning Handbook, 2nd Edition*
- *First Responders Guide to WMD, 2nd Edition*
- *Implementing Physical Protection Systems*
- *Personal Identification*
- *Professional Investigator's Manual*
- *Protecting Schools and Universities from Terrorism*
- *Readings in Security Management*
- *Security in 2020*

Schedule Your Professional Development Now

A comprehensive calendar is available here.Register early and save by taking advantage of early bird rates. Realize additional savings by booking your hotel room before the deadline. Plan ahead to get ahead.

Contribute to *AP Dynamics* and Earn CPEs



ASIS International invites members to submit articles to be published in future editions of *AP Dynamics*.

Articles that share knowledge and best practices with other ASIS members are welcome -- whether they are case studies, or articles about legislation in your own country, trends in security technology, or advancement in the security profession.

ASIS Board-certified professionals are entitled to claim up to nine CPE credits per article.

General writing guidelines:

- Articles must be in English only.
- Articles should not exceed 500 words.
- Sales or marketing submissions will not be accepted.

Please contact the editor for more information.

ASIS/IE Business School Executive Education Program: Learn to Be a Strategic Business Leader

IE Business School, Madrid

ASIS International will once again partner with Madrid-based IE Business School, one of Europe's leading business educational institutes, to deliver Effective Management for Security Professionals. This four-day, executive education program has been customized to introduce mid-to-senior level security practitioners to the dynamics of business fundamentals.

"The understanding of the 'bigger corporate picture,' and hence the business' security and risk management requirements, is key to implementing and managing an effective corporate security strategy, as well as ensure long-term support from senior management," states program graduate Michael Otto, corporate security officer, Novartis International AG. "The program and attendees' discussions provide guidance, as well as suggestions as to how best to achieve this objective."

Program participants will develop a strategic understanding of the role of security management as an enabler of business success and acquire the knowledge and skills needed to present a sound business case for their security initiatives.

The program will take place June 3-6, on the IE Business School campus. Preview the program and register to attend at www.asisonline.org.

Fees:

- €3.600 for ASIS members
- €4.500 for nonmembers

Registration:
Visit the IE Business School Program Web site to sign up.

Roy Bordes Award Application Now Open

The Roy Bordes Award for Physical Security provides the winning chapter with a customized, two-day, locally delivered, physical

security education program. Established in 2008, the award pays the cost of instructors, their travel and accommodations, and collateral materials. Award funds are limited, necessitating that additional meeting expenses will be the host chapter's responsibility. All chapters are invited to compete for the award, however, preference will be given to developing chapters working to expand membership and educational offerings. Chapters may submit one application annually. The award application period ends March 11.

Please click here for more information and eligibility criteria.

Application Period Open for University of Phoenix Full-Tuition Scholarships

Each scholarship will allow a prospective student to complete an undergraduate or master's degree program at University of Phoenix. Recipients may choose to attend a University of Phoenix physical campus or the University of Phoenix online.

Applicants must meet all admission requirements for the university and maintain good standing throughout the term of their scholarship. The scholarship is open to security practitioners worldwide.

A committee comprised of members from the ASIS International Board of Directors, ASIS Foundation Board of Trustees, and the ASIS Professional Certification Board will review applicants and select the scholarship recipients.

Applications will be accepted through April 15.

Please click here for more.

Headlines

Small Supply-Chain Partners Increasingly Targeted by Advanced Persistent Attacks

According to CSO Online, companies should not consider that their small size protects them from being targeted by the authors of advanced persistent attacks (APTs). These companies must consider themselves as the weakest link of larger supply chains.

Noting that APTs have become "a real and credible threat," BAE Systems Detica Asia-Pacific Head of Cyber Security Craig Searle warned that every part of a business supply chain needs to be protected equally. "The average SME might think they are not really of interest to an APT perpetrator," Searle said. "But it turns out that they're actually of great interest because the cyber-criminals are aware they don't have as much security control, as much robust technology, and process governance around security."

According to the article, companies with extensive supply chains do not believe that their partners' information security activities are effective. As a consequence, the importance of supplier security checks -- of both people and technology -- has grown and led to the inclusion of more prescriptive right-to-audit clauses into supplier contracts.

But Searle warned that it is difficult to implement the right controls if an organization does not have a clear understanding of their information assets, where they are, and what controls they have in place.

Source: CSO Online

Please click here for more.

First Asia-Pacific Cyber Intelligence Centre Opened

Future Gov Asia-Pacific reported that the first cybersecurity center of excellence in the region has been launched in Singapore by the Infocomm Development Authority (IDA), in partnership with Fireye.

In November 2013, Singapore was been targeted by cyberattacks. According to Jacqueline Poh, managing director of IDA, while the Singapore government was able to swiftly defend its digital assets, contain the attacks and apprehend suspects, it is important to be prepared for more serious, coordinated threats in the future.

In that respect, IDA will collaborate with FireEye to increase experts' skill levels. Secondly both organizations will work on the development of next-generation cyber-security solutions. IDA and FireEye aim to develop new solutions and products for both the local and regional markets.

"Organizations are coming to the rapid realization that they must be prepared to invest in building capability and capacity to deal with cybersecurity anytime, anywhere. If cyberattacks respect no borders, then defense must also be organized on a global scale," she said.

Source: Future Gov Asia-Pacific

Please click here for more.

Critical Sectors in India Get Cyber Attack Protection

The Indian government charged the National Technical Research Authority (NTRO) with securing critical infrastructures such as telecommunications, power, railways, and airports, Security Today reports.

The move was proposed by National Security Advisor Shivshankar Menon in December 2012 to shore up defenses against paralyzing cyberattacks in these sectors. But while

guidelines for the project were prepared and issued in June 2013, the government was caught in a furious battle over the project's ownership. While many felt the ideal choice was the Computer Emergency Response Team-India (CERT-IN), controlled by the Ministry of Communications and Information Technology, Menon was in favor of the NTRO, which is controlled by his office and is not answerable to Parliament.

In the first phase, the NTRO will look at seven sectors including telecommunications, oil and gas, air traffic control, power grids, nuclear installations, and railways. This phase will last five years. During this period, nearly 500 IT professionals with various levels of experience will be hired to start building robust defense systems for these sectors.

Source: Security Today

Please click here for more.

Increasing Mobile Traffic Volume in Asia-Pacific Will Increase CSOs' Security Burden

CSO Online reported that the predicted increase in mobile traffic volume will put some pressure on CSOs because the likelihood of mobiles being used as a vector for security attacks could rise.

This analysis follows the publication of the Cisco visual networking index global mobile data traffic forecast for 2013 to 2018. According to this report, mobile traffic volume in the Asia-Pacific region will grow by 67 percent annually through 2018, putting it well ahead of North America and Western Europe, which will each see 50 percent annual growth.

The report stresses that this trend could entail security issues as most customers do not want to pay for mobile security tools, despite ever-smarter mobile malware now intercepting phone calls and recruiting mobile devices into global botnets.

Cisco warns that another development should be taken into account by CSOs. An increasing trend towards WiFi-based mobile offload, which shunts mobile devices onto public or private WiFi connections to reduce overall loads on mobile networks, will see 52 percent of global mobile traffic pushed to WiFi networks, up from 45 percent of traffic last year.

That significant volume will see more mobile traffic traversing WiFi networks than mobile networks, forcing CSOs to ensure that their mobile-protection regimes are up to scratch, both on their own networks and outside of them.

Source: CSO Online

Please click here for more.

Eleven Pakistani Police Officers Killed in Suicide Bomb Attack

According to BBC News, a suicide bomber targeted a bus carrying Pakistani police officers that was leaving a police training center. The attack took place in Pakistan's southern city of Karachi and killed 11 police officers and wounded more than 40 others.

Hundreds of policemen have lost their lives fighting militants and criminal gangs linked to the city's main ethnic, political and sectarian parties, the BBC's Shahzeb Jillani reports.
The attack - which no one has yet claimed responsibility for - is one of the bloodiest on police in Karachi in recent months.

"Apparently an explosive-laden car hit the police van transporting officials," police official Muhammad Iqbal told the AFP news agency.

The latest attack comes amid talks between the government and the Pakistani Taliban to try and negotiate a peace deal.

Source: BBC News

Please click here for more.

Education and Events

Global Agenda

March 13-14, 2014 -- ASIS 24th New York City Security Conference & Exhibition, New York, USA
Registration is open!

April 1-3, 2014 -- ASIS 13th European Security Conference & Exhibition, The Hague, The Netherlands
Registration is open!

May 5-6, 2014 -- 7th Annual CSO Roundtable Summit, Miami, FL, USA

June 3-6, 2014 -- Effective Management for Security Professionals, Madrid, Spain

September 29 - October 2, 2014 -- ASIS 60th Annual Seminar & Exhibits, Atlanta, GA, USA

Professional Development

Webinars

Subscribe today and get all webinars FREE between now and December 31, 2014!

Webinar Archive

This month highlighting:

- Stop Issuing Secure Credentials to Imposters!
- Intimate Partner: Violence in the Workplace

Full list of archived titles

e-Learning

Full list of programs

Classroom Programs and Webinars

2014 at a glance.

ASIS ASIA-PACIFIC ADVANCING SECURITY WORLDWIDE. © 2014
To unsubscribe please contact the editor.