

TABLE OF CONTENTS

Article	1
Chairperson Message	2
Chapter Meeting	2
Article	4
Photo-article: Chapter Meeting – ASIS / Tyco International	5

NEW MAILING ADDRESS

ASIS International (Singapore Chapter) wishes to announce that with immediate effect, the mailing address of the Chapter has been changed to:

**No. 14, Robinson Road
#13-00
Far East Finance Building
Singapore 048545**

The old address will cease to be used with immediate effect.

ARTICLE SUBMISSION

Do you have an interesting article that you wish to share it with our members? Please email your article and write to the editorial management committee at newsletter@asis-singapore.org.sg

The Security Professional MICA(P) No. 183/02/2006 is published and distributed by the ASIS International (Singapore Chapter). While every care has been taken to ensure that all information in this newsletter is accurate, the publisher cannot accept and hereby disclaims any liabilities to any party caused by errors or omissions resulting from negligence, accident or any other cause. Editorial Management Committee: ASIS International (Singapore Chapter). The Secretariat is located at: No. 14, Robinson Road, #13-00, Far East Finance Building, Singapore 048545. Email: newsletter@asis-singapore.org.sg

PREVENTING TERRORIST AND CRIMINAL INFILTRATION OF VULNERABLE SITE BY UNDERSTANDING THE THREAT OF THE INSIDER

By Leonard Sng, CPP, CFS / Edited by Simon Lim, CPP

The paradigm of terrorism has shifted most significantly from one of inflicting critical damage to physical assets to the destruction of human capital. All with the intention of making governments and major commercial entities give in to the will of the terrorist. The World Trade Centre and Pentagon attacks in America in 2001, the Bali bombings of 2002 and 2004, the Madrid train bombings in 2003, the London Underground attack in 2005 and the botched attack of aviation at London Heathrow in 2006, all have one common denominator, the offering of high human traffic density. In view of this, it is therefore essential that risk management models take into account the human traffic density in their risk assessments when determining the vulnerability of their respective sites to an indiscriminate act of terrorism.

Limitations of Background Screening

The global security community recognized that there was an urgent need to review the background of persons employed at critical infrastructural sites. Screening against criminal registers did not offer much insight and there is an increasing need to make an attempt to identify the propensity for violence attributed to embracement of fundamentalist beliefs. The government of the United Kingdom in 2002 embarked on a rather ambitious initiative to subject all employees with airside access at airports to a background screening every 18 months. This initiative has been most challenging for the British Government as the number of employees with airside access at airports throughout the United Kingdom runs into the thousands with many migrant workers from South Asian countries.

With such regular background screening of employees working in the aviation industry in the United Kingdom in the last 4 years, it is probably now on the minds of policy makers as to how the background screening had missed one of the 21 suspects arrested in the botched terror plot at Heathrow in 2006, who was a security personnel with an all areas access pass at Heathrow Airport.¹ The British case highlights one of the major problems of background screening; depth of screening is inversely proportional to the massive number of employees screened.

While it makes good sense to incur much time, effort and cost to undertake comprehensive background screenings of persons seeking admission into boards of commercial entities, as we have seen with the case of Patrick Imbardelli, former Chief Executive for Asia Pacific of the Intercontinental Hotel Group.² It would certainly be an extremely demanding task of subjecting thousands of employees to a comprehensive screening protocol as was applied to Imbardelli.

The Validity Factor - Background screenings are only good for the present time that it is being done, such screenings have short validity periods and because of this the accuracy of such screenings are effected. It is also important to recognize that background screenings are only as good as the information that is captured in the database.

Chairman's Message



Dear ASIS Members,

Every year, Q3 has always been exciting for members of ASIS International. This year is no exception. On September 24th to 27th, more than 23,700 security practitioners participated in the very successful ASIS 53rd Annual Seminar & Exhibits held in glamorous Las Vegas. The security exhibition showcased latest state-of-the-art technologies and security tools offered by 950 exhibitors. As for the concurrent security seminar, 4,000-over delegates attended it to learn from security experts and business leaders including keynote speaker Tom Peters. In case you might have missed that event, I have provided a short write up in this issue of The Security Professional.

On August 9th, all Singaporeans celebrated our National Day with a wonderful parade on the new floating platform at Marina Bay. The economic progress, peace and prosperity that we enjoyed over the years are the result of the hard work of every Singapore citizen and a good government. We as security practitioners should be proud of that, and continue to play our part in our respective workplaces because corporate security and risk management are vital to sustain every successful business.

At a local Chapter level, on August 17th we had a fabulous Chapter Meeting of more than fifty members and guests at The Legends Club. During that event, we also presented book prizes to two very deserving graduates, Lye Chee Koon and Siva Jothi, from the recent Professional Diploma in Security Management course. Our heartiest congratulations to them! For more details of the event,

please see enclosed article by fellow Management Committee (MC) member Jeremy Khong.

Continuing with our fine efforts to provide security leadership and professional development opportunities, our Chapter participated in the Critical Site Security Summit conference and exhibition as a Supporting Organisation. That event organised by Asian Business Forum on 11th to 14th September provided a good platform for our association to showcase our certification programs and membership privileges. Our Chapter also had two MC members – Leonard Sng CPP, and yours truly – who delivered security presentations at the conference. We have provided an extract of Leonard's presentation in this newsletter, and we hope you enjoy reading it.

In the coming months, our Chapter's Management Committee will roll out some nice membership gifts for first-time new members as well as for membership renewals. So, don't miss out on it - renew your local Chapter membership early!

With Best Regards,

**Anthony Lee, CPP, CBCP
Honorary Chairman**

ASIS Information Resource Center (IRC)

New security resources have been added into the ASIS Information Resources Center (IRC) security catalog/database from May and June 2007.

This listing has been posted in the IRC Online section of the ASIS website (Click [here](#) for the link). Instructions for borrowing or accessing these materials are included.

Helen Yang
Librarian, Electronic Services and Resources
Information Resources Center ASIS International

ASIS International (Singapore Chapter) Q3 Chapter Meeting and Networking Event *By Jeremy Khong*

The Q3 ASIS International Singapore Chapter Meeting and Networking event was held on 17 Aug 07 at The Legends, Fort Canning Park and was organized in partnership with Tyco Fire, Security and Services Pte Ltd.

This event offered an opportunity for local chapter members to mingle with one another and interact with their peers in the security industry. Security professionals from various high profile organizations were present, together with representatives from the Singapore Police Force, namely SIRD (Security Industry Regulatory Dept) and GC (Gurkha Contingent).

Our Chapter Chairman, Mr Anthony Lee, kicked off the evening with the welcome address followed by the presentations of ASIS certificates to new members. Next was the presentation on "Physical & Electronic Security to Safeguard Facilities" by Messrs. Laird Hamberlin and Alan Parker, which provided a good insight into the usage of physical measures, combined with electronic systems to ensure the security of your facility. Most of the participants' tummies were growling with hunger by then & a sumptuous buffet dinner spread awaited them.

Mr. Henry Ang, a new ASIS member who attended the event said: "This presents an excellent opportunity for me to interact with fellow practitioners, catch up with acquaintances, as well as forge new relationships with potential vendors." ■

Continue from Page 1

A Necessary Limited Tool – Background Screening

Despite all these limitations of background screening it is still a necessary tool for companies and governments to consider it in employment selection. For effectiveness, such screenings should not stop at the pre-employment phase. Each time an employee is being considered for advancement to a more high-risk position, it is important that a background screening be considered. Each time there are signs of irregular behaviour displayed by an employee with high access, it is important to re-screen the person again and perhaps if the situation warrants and the law of the land permits, surveillance be mounted. The need to comply with the law of the land in undertaking covert surveillance should not be disregarded.

The Threat of the Insider

Terrorists are aware that with the hardening of security at key installations, it is difficult to undertake surveillance work on a casual basis. To be effective, you now have to sleep with the 'enemy'. The need for the 'Insider'; only with a well-placed source can terrorists gain much intimate and accurate information of their targets. Perhaps in some measure, we may have seen such a case in the July 2006 botched terror attack on aviation at Heathrow Airport.

Module 101 Of the World's Seconded Oldest Trade

While prostitution is known to be the oldest trade in the world, I believe not many are aware that espionage is the second oldest trade in the world and the second oldest trade employs in good measure the world's oldest trade. Espionage whether employed for commercial or for public purposes share one important characteristic, 'People', without which it would be difficult to infiltrate an organization let alone acquire privilege information. This has given rise to the practice of HUMINT or Human Intelligence. HUMINT occurs in three phases, the talent-spotting phase, the phase of cultivation and finally the recruitment phase.

Talent Spotting – This involves identifying people with the right access. Access need not be limited to direct privilege information; it also covers access to people with the access to privilege information. Taking a humble stand initially when discussing our access levels and our circle of acquaintances would be perhaps a way to evade the 'talent spotter'.

Cultivation – This is the most interesting and varied of the espionage cycle. The primary purpose of the cultivation is to better understand the subject more intimately and also confirm his level of access to information and key personnel in the organization. For instance, the propensity to lead a life of luxury, a compulsive gambling habit, weakness for women and alcohol are just some of the 'talents' that such talent spotters will be most interested to discover. The lesson to be learnt in here is that there is no such thing as a free lunch. The list of enticement is never ending and the cost of enticing a victim with the much-valued access is more than compensated when the victim is recruited and starts producing the required results.

Recruitment – When the subject target is assessed ripe for the picking, the process enters the recruitment phase. Here the cultivator would have acquired enough incriminating evidence to compromise the subject target. The recruitment

need not necessarily be so blatant and antagonistic. A good recruiter would be able to turn the situation around and make the subject feel that his sharing of privilege information is not going to do much damage to the company or the government. Furthermore, he is just performing the role of a consultant and he is paid a professional fee for his expert advice justified with hard evidence of course. Many agents on being recruited prefer to retain some pretence that they are 'merely a trusted source or that their information is for an elite international think tank rather than for another government or commercial conglomerate. This is called the 'fig leaf' and a surprising number of agents require this even though to all intents and purposes they are fully recruited and are conscious agents. Everybody knows what is going on, but nobody actually says so.³

If the recruitment proposal is refused, all is not lost. The key thing is not to pressurize the target. The last thing you want is an unwilling agent. There is always a chance that one day the target will need that help or that the fact that you didn't apply any pressure shows that you can be trusted.⁴

Possible Remedies to Social Engineering – Awareness

While most public and private entities would administer a security briefing to new employees, not very much effort is given to this insider threat issue. A starting point to counter the menace of social engineering or corporate espionage is to build a sufficient level of awareness among employees. This awareness development should not be a one off event but an on-going effort. Employees should be reminded of the threat of social engineering at least once every two to three years. This is so, as most social engineering initiatives take about six to eighteen months before the subject target becomes ripe for recruitment.

Knowing the threat of social engineering, it is equally important that employees be encouraged to adopt good information protection habits. Apart from maintaining such good information protection habits, employees with access to sensitive information should be advised to maintain a low profile. When the talent spotter is unable to associate an employee to have a high access level to information and to key management personalities, the subject employee becomes a less attractive target for the talent spotter.

A Counter Espionage Management Program – A Whistle Blowing Program

The way to prevent a company from being a victim of an espionage attempt is to have in place a 'Whistle Blowing Program.' As the term implies and to put it crudely, employees are encouraged to serve as informers on their superiors, peers and subordinates. This will only work when employees who whistle blow are assured of their confidentiality and will be protected from any form of prosecution.

To put in place a whistle blowing program, there is a need for some structure as to how it should be administered and who should have access to knowing the identities of the informer or the whistle blower. However, for informers to give their identities away, they must be assured of their confidentiality at all cost. Once there is a failure in protecting the confidentiality of an informer, to resurrect the whistle blowing program would be near impossible.

Continue at Page 4

ASIS INTERNATIONAL 53RD Annual Seminar & Exhibition

by Anthony Lee, CPP, CBCP

Of all the ASIS International Annual Seminar I have attended, this one is certainly the most successful. More than 23,700 security practitioners attended the exhibition that showcased the cutting-edge technologies, products and services offered by 950 exhibitors. Also 4,000 over delegates attended the security seminar. ASIS Singapore Chapter is represented by Honorary Chairman Anthony Lee, CPP; Paul Rachmaidi CPP and several others. As always, the seminar provided a comprehensive educational program – more than 155 sessions in all – ranging from Convergence of Enterprise Security, Developing a Security Master Plan, Security Architecture and Engineering, Security Metrics Measurement, to name but a few.

President's Reception

As expected the President's Reception was well attended by a variety of delegates, meeting up with old friends and making new ones. This personifies one of the many benefits of membership of ASIS International, networking with professionals from diverse environments, sharing experiences, generally catching up with issues affecting different people and most of all enjoying the company of people who are passionate about the security profession in a social environment.

Key Note Speaker: Peters Promotes Excellence

People and excellence. If keynote speaker Tom Peters had his way, these would be the only two terms in every businessman's vocabulary. It doesn't matter what your business is, these are the two things every business needs for success whether you make widgets or provide security.

"Being good at what you do is not about the toys, but about the people," said Peters in his emphatic, no-nonsense manner. Peters said what every security person must know innately: No one remembers your wins, but everyone will remember your losses. Because of this, security professionals should remember one name, Charles Darwin, and follow his iron law of nature: Be adaptive.

One area Peters zeroed in on was the security industry's proclivity to say "security" way, way too much. You are risk managers, said Peters. Positive reinforcement is everything in business. Be positive and people will respond. Remember, perception is everything, Peters reminded the audience.

In a business marked by terrorism, disasters, and the worst humanity can throw at you, security professionals must emphasize its successes. "You teach people by bringing up good stories," says Peters. Security managers, like any business executive, should also remember their staff is everything. "Unearth the champions," Peters stressed.

Closing Ceremony

The final event of the conference was the closing luncheon with a talk by Christopher Gardner. A passionate philanthropist and owner/CEO of an international brokerage firm, Gardner shared his rags-to-riches story – from homelessness to Wall Street. You may have seen the recent movie, *The Pursuit of Happiness*, or read his autobiography, both inspired by his amazing life. One thing is certain – you will never forget Gardner's remarkable story of struggle, faith, entrepreneurialism, and fatherly devotion.

For me and many other people who attended the ASIS International Seminar and Exhibits, it was an immensely successful event. We can certainly look forward to even bigger things at next year's ASIS International event in Atlanta, Georgia. ■

Continue from Page 4

For confidential reporting to be effective it must only have one recipient, for instance in our context the Corporate Security Director should be the one opening, reading and following up on the confidential report. He must be able to compartmentalize the operations effectively and it may be necessary to assign a pseudo-name or code name to the employee who submitted the report. If interviewing the informer is necessary, this should be done outside the company and effort should be taken to make sure that the meeting is not being watched.

Conclusion

Companies and Government agencies must recognize that they can fall prey to espionage. This recognition is the first step in being prepared for an espionage attack on the organization. To understand how susceptible the organization is to an espionage attack, it would be advisable that the threat of espionage be incorporated into the risk analysis protocol adopted by the organization. Having an awareness program for employees that drives the message home when they first

join the company and making it a point to re-visit the topic once every 3 to 5 years dependent on how vulnerable the establishment is to being targeted for espionage would be the next step to take. To avoid having to come to the point of having to remedy an espionage attack, a whistle blowing program would help deter espionage, as employees are encouraged to report on staff and be assured of complete confidentiality. We cannot totally eliminate this menace; espionage is the world's second oldest trade and will continue to exist as long as there is privilege information to be acquired. Espionage is motivated by opportunity and will seize the day when an organization lets its guard down.

References

1. *CNN.com – Agent Infiltrated Terror Cell, U.S. Says – Aug 10, 2007.*
2. *The Singapore Straits Times – Top Hotelier Caught Lying in CV Resigns – Jun 16, 2007*
3. *Harry Ferguson – BBC Spy Handbook – Case Study: A Typical KGB Recruitment, Pg 104 – 114.*

This paper was presented by Leonard Sng, CPP, CFS during the Asia Critical Site Security Summit organised by Asian Business Forum from Sep 10 to 12, 2007.

ASIS SINGAPORE CHAPTER GATHERING

17th August 2007 @ The Legends Fort Canning

In partnership with Tyco Fire, Security & Services Pte Ltd



Photographs Contributed by Jeremy Khong