Countering the Insider Threat

An Introduction to Personnel Security
THE TRAINER

Andrew Peck

British Army Intelligence Corps
1965 – 1987

Head of Security London Marriott Hotel
1987 – 2004
SECURITY THREATS
SECURITY THREATS
COUNTERING THE INSIDER THREAT

AN INTRODUCTION TO PERSONNEL SECURITY
WHAT IS PERSONNEL SECURITY?

A system of policies and procedures, which seeks to manage the risk of staff or contractors exploiting their access to the organisation’s assets for unauthorised purposes.

Those who seek to exploit their legitimate access are referred to as "Insiders"
WHAT WILL WE BE COVERING IN THIS PRESENTATION?

What?
What is the Insider Threat?

Why?
Why do they do it?

Who?
Who is an Insider? How do we spot them?

How?
How do we counter the threat?
THREATS TO THE SECURITY OF OUR VITAL ASSETS

- INFORMATION THEFT
- PROPERTY THEFT
- SABOTAGE
- TERRORISM
THEFT OF INFORMATION

ESPIONAGE
Chapter 13 – The Use of Spies

There are five classes of spy:

5. Local spies
6. Inward spies
7. Converted spies
8. Doomed spies
9. Surviving spies
Chapter 13 – The Use of Spies

There are five classes of spy:

2. Inward spies (making use of officials of the enemy)
Комитет Государственной Безопасности

KGB
COLD WAR – 1945-1992
INSIDERS WORKING FOR THE SOVIET UNION

In 1962 John Vassall, a clerk in the Admiralty, was arrested and charged with espionage. He had been recruited by the Soviet KGB in Moscow in 1954.

During his career as an “insider”, he passed thousands of secret documents to his case officers, providing information on British radar, torpedoes and anti-submarine equipment.
INSIDERS WORKING FOR THE SOVIET UNION

Aldrich Ames – CIA Operator
Worked as an Insider from 1985 - 1994

Received total of $4.6 million
Passed several lie detector tests
Eventually arrested because of his lavish life style
INSIDERS WORKING FOR THE SOVIET UNION

Robert Hanssen – FBI Agent
Worked as an Insider from 1979 – 2001. 22 years.
Received a total of US$1.4 million.
In 1982 the ISD exposed and expelled two Russian spies for espionage activities in Singapore.

Anatoly Alexeyevich Larkin a Soviet military intelligence officer, attempted to cultivate an Army 2Lt to conduct espionage against the SAF.

More recently, the ISD detained 2 persons in 1997 and another 4 in 1998. All of these were controlled agents of a foreign intelligence service.
SINGAPORE ESPIONAGE

ISA ARRESTS OVER PAST 2 YEARS

6 held for espionage

SIX people were arrested and detained without trial for espionage activities in the last two years.

Four have been released, and investigations against the other two are continuing. Home Affairs Minister Wong Kan Seng disclosed on Wednesday in a written response to a question from Nominated MP Simon Tay.

Under the Internal Security Act, those suspected of being involved in activities that might threaten national security were arrested. Two were arrested in 1997, and have since been released. One of them, a male Singapore Permanent Resident, was a deep-cover operative of a foreign intelligence service, and had used the other, a female Singaporean, as a collaborator.

Of the other four male Singapore citizens detained last year, three were agents in another intelligence service. One had recruited the fourth to collect intelligence on and to subvert an unknown department's recommendations that their preventive detentions were no longer necessary for reasons of continuing investigation, or of their posing an active threat to national security.

The four who were released from custody had been detained for between four and 11 months.

Since 1965, 591 people have been detained under the Internal Security Act. Most were arrested in the 1960s and early 1970s.
THEFT AND FRAUD FOR FINANCIAL GAIN
Christmas Day 2008
Jerry Ee, senior supervisor at Cortina Watches, returned to the shop after it had closed for the day. He had two large suitcases with him. After packing, he was picked up in a rented limousine and taken straight to Woodlands checkpoint. He had with him over 360 luxury watches and cash worth over S$7.7m.

After living it up with a friend in Thailand for three months, Jerry surrendered to police, and was subsequently convicted and sent to prison in Singapore for nine years.
Securitas Cash Handling Depot, Tonbridge, Kent, UK
2006
Tuesday 21 February 2006, 1828 GMT: Colin Dixon, manager of a Securitas depot, is stopped by bogus police officers at Detling, Kent.

1945: Mr Dixon arrives at Elderden Farm, near Staplehurst, Kent.

2020: Two other bogus police officers arrive at the Dixon family home in Herne Bay, Kent and take away Mr Dixon's wife, Lynn, and a young child.

2145: Mrs Dixon and the child arrive at Elderden Farm.
Wednesday 22 February, 0128: Mr Dixon is taken to the Securitas depot at Tonbridge, where he is forced to gain entry for the robbers.
ROBBERY IN PROGRESS
ROBBERY IN PROGRESS
ROBBERY IN PROGRESS

Made possible by the use of an insider, an employee deliberately planted in the depot to provide information on the security systems, methods of operation, personal routines of the staff.

Miniature camera disguised as a belt buckle.
INSIDER FRAUD
INSIDER FRAUD

The UK anti-fraud agency, CIFAS, recently did a survey of 127 companies, and found that only 2 claimed not to have experienced any insider fraud.

The larger companies were dismissing on average over 100 employees each per year for offences of this type.
Case History:

Project manager in the social housing sector set up a company owned by himself. He then awarded a contract to the company, and during a three-week period submitted invoices for the installation of kitchens that never took place.

Total of 15 invoices were submitted, relating to over 300 properties, at a cost of over UK£2million.
INSIDER FRAUD

Directors
Senior Management
Managers
Supervisors
Clerical / Administrative staff

Trust
Control
Value
INSIDER FRAUD

Typical frauds committed by more senior staff:

- Setting up false suppliers.
- Authorising contracts with companies supplying goods or services in return for kickbacks.
- Embezzlement of company funds.
- Placing fictitious staff on the payroll.
- Falsifying sales figures to increase bonus payments.
- Moving funds from client accounts.
INSIDER FRAUD

Junior staff often have just as good access.

Case History:

Credit card issuer had 60 cards stolen, with losses of $1m. Cards meant for overseas customers were sent out with insufficient postage, and were returned to the card issuer. A junior member of staff responsible for handling returned mail was keeping the returned cards and then selling them externally. The staff member had been recruited by criminals in a night club.
INSIDER FRAUD

Staff have even been recruited as they go for their smoke in the street outside the office staff entrance.

In recent survey of UK bank industry, 78% of those sacked for fraud were under 30 years old. Only 4% were over 41 years old.
INSIDER FRAUD

Does that sort of thing happen in Singapore?
Singapore Land Authority (SLA)
Deputy Director of Technology and Infrastructure Department
Koh Seah Wee
Allegedly rendered false invoices for fictitious maintenance contracts in transactions between January 2008 and March 2010, worth $11.8 million.
THE TERRORIST INSIDER

Bombing of the Jakarta Marriott and Ritz-Carlton 2009.

On 17 July 2009, two bombs exploded 5 minutes apart, the first in the Marriott and the second in the Ritz-Carlton.

7 people were killed, plus the 2 suicide bombers.
Bombing of the Jakarta Marriott and Ritz-Carlton 2009.

The bombing was planned by Noordin Top.

But the key player was a man named Ibrohim. Ibrohim was a florist who worked for a florist company with stores in both hotels.

He had been recruited into Noordin Top’s group in 2000.
THE TERRORIST INSIDER

Bombing of the Jakarta Marriott and Ritz-Carlton 2009.

As the insider, Ibrohim’s role was crucial.

He carried out surveys of both hotels, provided information on security measures, and smuggled the bombs into the hotels.

The bombs were smuggled into the hotels the day before the attack. They were brought in through the Marriott loading dock in a pick-up truck rented by Ibrohim.
Bombing of the Jakarta Marriott and Ritz-Carlton 2009.

The bombs were then detonated by two suicide bombers who had checked in as paying guests.

Dani Dwi Permana, Marriott

Nana Ikhwan Maulana, Ritz-Carlton

A third bomb failed to explode and was found in Marriott room 1808.

Ibrohim was killed by Indonesian police a few days later.
Major Nidal Malik Hasan

US Army psychiatrist. On 5 Nov 09, entered his workplace in Fort Hood, Texas, and opened fire with a pistol on soldiers there. He fired over 100 rounds, killing 13 people and wounding 30.

Trial still not taken place, but it seems that Major Hasan had developed extreme religious and political views.
SUMMARY OF INSIDER MOTIVATION

➢ Personal gain.

➢ Personal grudge.

➢ State-sponsored or corporate espionage.

➢ To make a political or ideological statement.

➢ To further the aims of a terrorist organisation.
SUMMARY OF INSIDER MOTIVATION

Deliberate penetration with general or specific intention of abusing position

Opportunistic exploitation of access once in post

Exploitation by others once in post
SO, WHAT CAN WE DO ABOUT IT?
PERSONNEL SECURITY FRAMEWORK

Stage 1:
Personnel security during recruitment

Stage 2:
Personnel security during employment

Stage 3:
Personnel security on leaving employment
Aim of Pre-employment screening:

- To detect individuals who might be deliberately joining our organisation with the intention of exploiting their access.
- To detect individuals with personal characteristics or circumstances which would make them vulnerable to exploitation by an outsider.
PRE-EMPLOYMENT SCREENING

Do we need to screen everyone?

- Should be an integral part of your policies, procedures and practices for the recruiting and hiring of new employees.

- Our personnel risk assessment will help us decide the level of screening appropriate for each post.
## PRE-EMPLOYMENT SCREENING

### What do we want to know?

- Identity
- Educational history
- Employment history
- Financial / Criminal record
How to verify identity

The most common methods for verifying identity are:

- Checking a person’s details against external databases – the ‘electronic’ approach.

- Requesting original documents – paper-based checks.
PRE-EMPLOYMENT SCREENING - IDENTITY

Paper-based Checks

- NRIC
- Passport
- Utility bills, bank statements
PRE-EMPLOYMENT SCREENING - IDENTITY

Even in Singapore impersonation is quite common

"BANKRUPT TRIED TO ENTER CASINO USING WIFE'S IC"

"MAN USED WORK PASS TO ENTER CASINO"

"MAN USES BROTHER'S IC TO GET INTO CASINO"

"23-YEAR-OLD IMPERSONATES FRIEND TO HELP HIM WITH IPPT"
Paper-based and electronic both have their key advantages.

For some posts, a combined approach is probably best.

This will allow you to verify the applicant’s original documentation, and benefit from the comprehensiveness of the electronic approach.
Qualifications:

Educational certificates are often much easier to forge than national identity documents.

Compare course titles, dates, grades, etc, with details given by the applicant.

Contact the establishment concerned, or at least do an internet check, to compare the logo, crest, contact details with those on the certificate.
OVER 400 foreigners were caught last year for lying to the Manpower Ministry in their work pass applications, a fourfold increase from the previous year.

MOM did not give a breakdown but the majority are believed to have used fake or forged qualifications in applying for employment passes which are for highly qualified people, or S-Passes for semi-skilled workers.
Immigration and Checkpoints Authority figures also point to a rising trend of workers using qualifications from degree mills, which are bogus universities that sell degrees for little or no study.

While most of those found out so far are foreigners, experts warn that more Singaporeans are also beefing up their resumes with fake or forged degrees.

One indication: The names of 36 people from Singapore showed up on a list of 9,612 people exposed in the United States recently for having bought fake diplomas and degrees.
IntegraScreen, which does screening work for the immigration authorities in several countries in Asia and the Middle East, said about 5 per cent of the resumes they screen are found to be fake.

Its managing director, Mr John Baxter, said: 'The use of diploma mills is exploding as the Internet makes buying bogus degrees easier than ever before. More workers are buying these degrees because they're looking for an edge in the competitive job market in Singapore.'
Almost any degree, from aviation to zoology, can be purchased. All it takes is a credit card number and computer access.

Most degree mills charge between US$50 and US$5,000 (S$69 to S$6,900) for degrees at all levels. Often, buyers only have to fill up a form stating their work and life experiences and pay up.

Within a week, they are sent a professional-looking degree scroll and transcripts of fictional grades to show potential employers.
University Degree

OBTAIN A PROSPEROUS FUTURE, MONEY-EARNING POWER, AND THE PRESTIGE THAT COMES WITH HAVING THE CAREER POSITION YOU’VE ALWAYS DREAMED OF. DIPLOMA FROM PRESTIGIOUS NON-ACCREDITED UNIVERSITIES BASED ON YOUR PRESENT KNOWLEDGE AND PROFESSIONAL EXPERIENCE.

If you qualify, no required tests, classes, books or examinations.
These are real, genuine degrees that include:
Bachelors, Masters, MBA and Doctorate Degrees.
They are fully verifiable and certified transcripts are also available.

Confidentiality Assured

1-650-xxx-xxxx
24 hours a day, 7 days a week including Sundays and Holidays
PRE-EMPLOYMENT SCREENING - EDUCATION

THE TRINITY COLLEGE
AND UNIVERSITY
PART OF THE EDUCATIONAL DIVISION OF
THE UU, INCORPORATED IN DOVER, DELAWARE

HAS CONFERRED UPON
Aamir Liaquat Hussain
THE DEGREE, RANK and ACADEMIC STATUS
Bachelor of Arts
in
Islamic Studies

ALL REQUIREMENTS of the BOARD OF
REGENTS and EXAMINERS HAVING
BEEN SUCCESSFULLY COMPLETED,
ALL RIGHTS and PRIVILEGES THEREunto
APPERTAINING ARE HEREBY AWARDED.
(Serial No. 00212117)

SIGNED and SEALED UPON THIS DAY
17th March, 1995
Dean of Studies.

ROYAL MELBOURNE
INSTITUTE OF TECHNOLOGY

This is to certify that
was admitted to the Degree of
Bachelor of Business
(Marketing)
with Distinction
on the twenty-seventh day of August in the year 2005
having completed an approved program of study

Chancellor of the University
Vice-Chancellor of the University

AETOS

YOUR SENSE OF SECURITY
Employment:
As with the qualifications check, the main aim of the employment check is to verify the information provided on the application form. The period checked should be at least 3 and preferably 5 years. The verification focuses on the following:

- Dates of employment
- Positions held
- Duties
- Salary
- Reason for leaving
Employment:

If the applicant presents pre-prepared references, you are advised to confirm that they are genuine. For example:

- Check the existence of the employer.

- Telephone the author to confirm that he provided the reference. The telephone number should be obtained independently – do not rely on that supplied by the applicant.
PRE-EMPLOYMENT SCREENING – CRIMINAL HISTORY

Criminal Convictions:

➢ Does the post require the applicant to be free of all criminal convictions?

➢ If not, what are the criteria, or who makes the decision on whether to employ or not?

➢ Certain offences can be considered ‘spent’ after a period of 5 years from the date of the offence (Registration of Criminals Act)
Criminal Convictions:

Information on criminal convictions can be obtained by:

- Asking the applicant to complete a self-declaration.
- Request a check via an external agency.
PRE-EMPLOYMENT SCREENING - FINANCIAL

Financial Checks:

In some posts, it may be justifiable to carry out financial checks.

- Bankruptcy
- Level of debt
Financial Checks:

- Self-declaration
- External agency checks
PRE-EMPLOYMENT SCREENING

Find us on Facebook
PRE-EMPLOYMENT SCREENING

Interview
PRE-EMPLOYMENT SCREENING

- Ask his reasons for wanting to join the company.
- Question him on any gaps in his educational or employment history.
- Does his verbal story agree with the written record.
- Are there elements in his private life that might indicate a vulnerable personality?
- Do you feel comfortable with the person?
PERSONNEL SECURITY FRAMEWORK

Stage 1:
Personnel security during recruitment

Stage 2:
Personnel security during employment
SUMMARY OF INSIDER MOTIVATION

Deliberate penetration with general or specific intention of abusing position

Opportunistic exploitation of access once in post

Exploitation by others once in post

On-going Personnel Security

Pre-employment Screening
ONGOING PERSONNEL SECURITY – POINTS TO CONSIDER

- Security Culture
- Line management
- Countering manipulation
- Ongoing screening
- Reporting suspicions
- Secure contracting
- Controlling employee access
- Controlling employee IT access
- Monitoring employee access
- Investigation
SECURITY CULTURE
SECURITY CULTURE

HARD WORK NEVER KILLED ANYONE BUT WHY TAKE THE CHANCE

AETOS
YOUR SENSE OF SECURITY
SECURITY CULTURE

Some organisational cultures may not be supportive of appropriate security behaviours
SECURITY CULTURE

Examples of poor security behaviours:

- Security cupboards not closed or locked.
SECURITY CULTURE

Examples of poor security behaviours:

➤ Employees not wearing passes.
Examples of poor security behaviours:

➢ Security passwords being shared.
Survey undertaken by the organisers of Infosecurity Europe 2003:

The most common password was “password” (12%).

The most common category was their own name (16%), followed by their football team (11%) and date of birth (8%).

Two-thirds of employees had shared their password with a colleague in the past year, and three-quarters claimed to know at least one co-worker’s password.
Examples of poor security behaviours:

- Sensitive documents being left out on desks.
SECURITY CULTURE

Examples of poor security behaviours:

➢ Employees not logging out of terminals.
SECURITY CULTURE

Why does it matter?

What has it got to do with detecting insiders?
SECURITY CULTURE

- Security procedures are there so that access to our assets is restricted to those who NEED access.

- If a person tries to get unauthorised access to an asset he must break one or more of the rules and thereby draw attention to himself.

- If EVERYONE breaks the rules, all the time, and no-one cares, then the real ‘insider’ will not be highlighted.
SECURITY CULTURE

An organisation must have a clear idea of the security culture it wants.

The styles, approaches and values that an organisation wishes to adopt towards security.
SECURITY CULTURE

Principles of culture management:

3. Good communication – clear explanations (briefings) to all concerned.

5. Management support – modelling of the desirable behaviours, especially by senior managers.

7. Clear policy and procedures – consistent implementation of the system.

9. Individual responsibility.
ONGOING PERSONNEL SECURITY – POINTS TO CONSIDER

- Security Culture
- Line management
- Countering manipulation
- Periodic reviews
- Secure contracting
- Controlling employee access

- Controlling employee IT access
- Monitoring employee access
- Reporting suspicions
- Investigation
PERSONNEL SECURITY FRAMEWORK

<table>
<thead>
<tr>
<th>Stage 1:</th>
<th>Personnel security during recruitment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 2:</td>
<td>Personnel security during employment</td>
</tr>
<tr>
<td>Stage 3:</td>
<td>Personnel security on leaving employment</td>
</tr>
</tbody>
</table>

AETOS

YOUR SENSE OF SECURITY
EXIT PROCEDURES
EXIT PROCEDURES

CASE STUDY
In November 2001, Vitek Boden was sentenced to two years in prison for releasing up to one million litres of sewage into a river and the coastal waters of Maroochydore in Queensland, Australia.

Boden had previously worked on the Maroochydore water project as a consultant but had been refused a full-time job by the Maroochydore local government. He used the internet, a radio transmitter, stolen software and his inside knowledge to carry out the attack.
EXIT PROCEDURES

CASE STUDY
Omega Engineering – United States.

Angered by his termination, a computer-systems administrator crashed Omega's companywide server and stole vital backup files. Production ground to a halt. Despite the best efforts of a team of data recovery experts, Omega lost about $10 million and countless files.
EXIT PROCEDURES

➢ Employees leaving an organisation take considerable knowledge about operations, assets and security vulnerabilities with them – possibly to a competitor.

➢ Circumstances of their leaving are not always amicable.

➢ A formal, thorough procedure for staff departures is required to ensure appropriate actions are taken to protect the organisation.
EXIT PROCEDURES

As soon as a line manager becomes aware that an employee is leaving he should assess the risk to the organisation from that person leaving.

- Is it voluntary, the result of disciplinary action or retrenchment.
- If they are not leaving voluntarily, the reason for dismissal.
- Where are they going to work next (e.g. a competitor?).
- Their current role and level of access.
EXIT PROCEDURES

Having assessed the risk, determine the best next course of action. Generally, the options will include:

- Allowing the employee to carry on working normally during their notice period.
- Allowing the employee to work their notice period but with reduced access.
- Asking the employee to leave immediately – possibly under supervision to prevent any unauthorised act while still on the premises.
## EXIT PROCEDURES

### ITEMS TO BE RETURNED

- Uniform
- Security pass/ID
- Mobile/Blackberry/Pager
- Company credit card
- Any unused name cards
- Keys/electronic access cards
- Books, papers, documents
- Laptop and any accessories
EXIT PROCEDURES

PREVENT FUTURE ACCESS (PHYSICAL AND ELECTRONIC)

- Blocking the employee’s user IDs
- Changing passwords to common systems
- Cancelling the employee’s electronic card access.
- Changing door PIN codes to common areas.
- Changing combination lock settings, if applicable.
- If necessary, issuing instructions to security guards.
RECAP

THE PRESENTATION HAS BRIEFLY COVERED:

- What is the Insider Threat
- Motivation and methods of the Insider
- How to counter the threat
INTRODUCTION TO AETOS

• **Formed in Apr 2004 via merger of:**
  - PSA Police
  - ST Kinetics Police
  - CIAS Police

• **Leading security service provider in Singapore**

• **100% owned by Temasek Holdings**

• **Current staff strength of 2,800**
AETOS SECURITY TRAINING & CONSULTANCY
Providing a wide range of security training and consultancy services

andrew.peck@aetos.com.sg

sophiatan@aetos.com.sg
Any Questions?