AIPIO
2012 National Road Show

Counter Intelligence: using the forgotten intelligence

 1

Outline

Session 1 Contemporary CI

Session 2 Hostile Intelligence Gathering

Session 3 Designing & Making the Case for a CI Programme

Session 4 Technical Security

Concluding remarks

 2

Buzz Words

- Intelligence
- Counter intelligence
- Counter espionage
- Espionage
- Business intelligence
- Competitive intelligence
- Industrial espionage
- Economic espionage
- Corporate intelligence

 3

Intelligence

Definition

- "*Information that has been analyzed and refined so that it is useful to policymakers in making decisions*".

Intelligence Cycle

Source: NZSIS

 4

Session One

CONTEMPORARY CI

 5

Counter Intelligence

- Offensive (CE)
- Defensive
  - Counter hostile intelligence collection by adversary
    - HUMINT
    - SIGINT
- Forgotten ?
- CI ≠ Protective Security

 6

Change

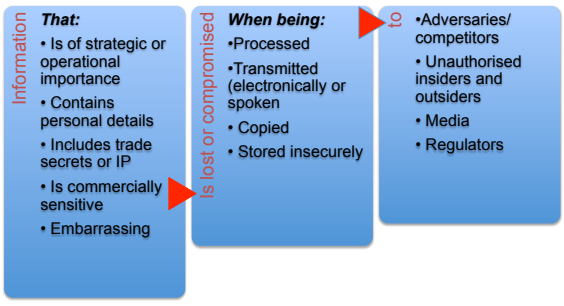
1928 - 2011

- "*The biggest mistake we could make would be to miss the changes*"
  - Glenn Whidden (1990)
- Changes to:
  - Adversary capability
  - Technology

 7

Intelligence Cycle Protection

 8

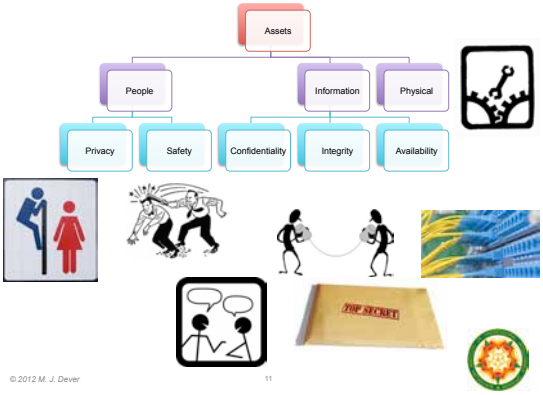


 9

CI Survey Process

- ID Assets
- Threat assessment
- Vulnerability
- Asses risk (SRA)
- Identify and analyse options
- Choose measures
- Write operational requirements
- Implement
- Monitor
- Review

 10



 11

CI Adversaries

- FIS
- Organised Crime
- Corporations
- Individuals
- Groups
- Media

 12

Session Two

HOSTILE INTELLIGENCE GATHERING

 13

 14

Covert Collection

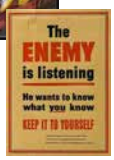
Hey boss. I'm not sure our covert surveillance is real covert any more.

- Means to an end
- Leisurely
- Legal ?
- Ethical?

- Adversary needs:
  - Access
  - Time
  - Money

 15

Methods



HUMINT

Technical Collection

 16

Session Three

DESIGNING & MAKING THE CASE FOR A CI PROGRAMME

 17

 18

Risk Assessment

High Impact Low Probability	High Impact High Probability
Low Impact Low Probability	Low Impact High Probability

- Threat
- Vulnerability
- Impact (Business Impact Level)

 19

Risk Acceptance & Tolerance

 20

Threat Assessment

- Basis for smart security decisions
- Threat is a matter for intelligence

 21

Targets

- Any one with influence, money, power or access to valuable, sensitive or classified information…..
  - Holders of High Office
  - Senior executives (public & private)
  - Celebrities, Royalty
  - Law enforcement officials
  - Lawyers
  - Spouses, neighbours ……

 22

Motives

- Economic crime
- Organised crime
- Competitive intelligence
- Corporate espionage
- Disgruntled or issue motivated
- Terrorism
- Extortion/harassment
- Internal intrigue
- Media snooping
- Personal privacy invasion/stalking

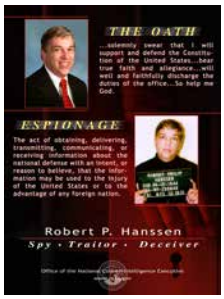
 23

Capability

- Time
- Access
- Money

 24

Insider Threat



 25

Vulnerability Assessment

Who will be the first to test your security measures?

 26

Counter Intelligence Strategy

Key Elements

- Senior management endorsement
- Awareness program
- Compliance
- Protective security
- TSCM surveys

 27

Session Four

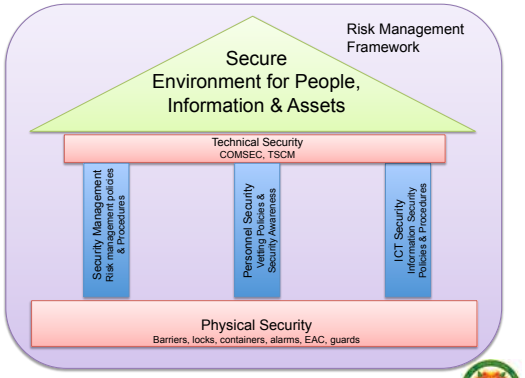
TECHNICAL SECURITY

 28

Technical Security

- Measures taken to prevent, deter, and detect intelligence gathering by electronic, electromagnetic, oral, visual and other means
- Technical security is NOT ICT security

 29



 30

Eavesdropping

- **Direct** (or acoustic)
  - Airborne
  - Structural
- **Assisted**
  - Listening devices
  - Communications monitoring



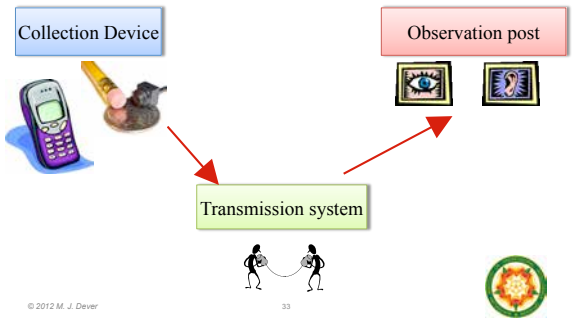
 31

Technical Surveillance Threats

- Listening devices
  - Wired
  - Wireless
  - Esoteric
- Imaging devices
  - Visible
  - Invisible
- Tracking devices
  - Passive
  - Real time
- Interception
  - Telephone
  - Fax
  - Keyboard loggers

 32

Basics of Technical Surveillance

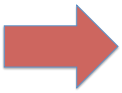


 33

Visual Surveillance

 34

Analogue to Digital



3G
4G
WLAN

 35

Interception

- Telephone systems
  - Wired
    - Analogue
    - Digital (VOIP)
  - Wireless
    - Cordless
    - Cellular
  - Fibre
- Two way radios
- Intercommunications

 36

Tracking



 37

Evolving audio threats



1920's 1970's Now

 38

Evolving video threats

1962

Now

 39

TSCM Surveys

Definition

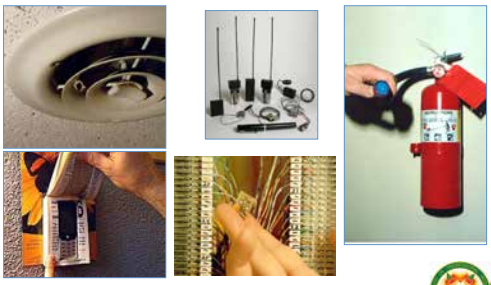
- A systematic physical, electronic and visual examination of a physical item or place by a *qualified specialist* in order to detect technical surveillance devices, technical security vulnerabilities and related physical weaknesses

Protocol

- SRA
- Physical search
  - Vulnerability ID
  - Audio conduction tests
- Electronic search
  - Electromagnetic spectrum
  - Communications systems
  - Building wiring systems and elements
- Anti tamper

 40

Needle in a Haystack?



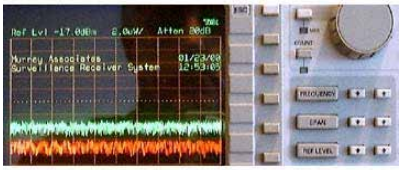
 41

TSCM Equipment

 42

TSCM Specialist

Instrumentation is nothing...



Courtesy Spybusters.com

without the right reflection in the screen.

 43

"There are fine cigars and cheap cigars, but there are no fine cheap cigars"

Winston Churchill

 44