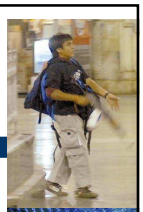
Human Bombs Inside an Organization

Naavi
Information Security Consultant
21st May 2010

Security Landscape



- Visible threats
  - Attacks with guns, bombs and mines
    - Physical Security Domain
- Facilitated by digital surveillance, reconnaissance and guidance
  - Information Security Domain
- Third Dimension
  - Supported by human agents within the target community
    - Behavioural Science Dimensions
      - Insider Threat Dimension

ChangingThreat Scenario?

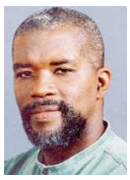
- A Truck laden with explosives ramming into the building.. Is a known risk
  - The company driver driving the CEO's wife and children in the Car..
    - With RDX in the boot… possible?
      - Are we ready for such insider threats?

Terrorist Plots and Insider Involvement

- In 2007, Report prepared by FBI and Critical Infrastructure Threat Analysis Division of US found
  - Al-Qa'ida planner Dhiren Barot, whom UK authorities arrested in 2006,
    - had tasked a member of his group to secure employment at a hotel in the UK to learn how to deactivate fire and security systems
      - In 2008, 26/11 happenned..terrorists had complete information on the interors at Taj..suspected to have served as employees

Terrorist Plots and Insider Involvement..2

- Russel Defreitas, the alleged mastermind behind a plot to explode jet fuel pipelines at John F Kennedy International Airport, New York
  - had been a cargo handler at the airport.
    - used his job related knowledge to conduct surveillance and plan the attack
  - Was a similar plot in store in Cochin?



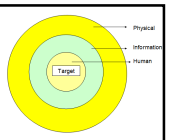
Rajiv Gandhi Assasination

- Nalini facilitated Sivarasan and others
  - Without Nalini's logistic support the terrorist act would have failed to take off

We Require a an appropriate strategy ..

..to defuse the human bombs ticking inside an organization

PIH Approach to Security



A holistic security approach which combines Physical, Information and Human aspects of securing a target

Problem is grave …

Solution has to be ruthless…

Solution is..

Identify the human risk and …Mitigate

Strategies for Mitigation of Human Risks

Suggested Policies and Practices

Threat Mapping

- Step I
  - Identify employees who have a propensity for deviant behaviour
  - Classify them as probable, potential, real threats and
    - initiate apropriate actions

Threat Mapping..2

- Step II
  - Observe and update information
  - Double check background
  - Review until the classification is crystallized

Threat Mitigation

- Step III
  - Initiate Corrective Action Plan
    - Real Threats
      - Keep Away
    - Potential Threats
      - Avoid sensitive positions and tag for surveillance
    - Probable Threats
      - Correct through self improvement Behavioural Training programmes
        - to sensitize them on their negative tendencies and help them correct it themselves

Requires HR to work closely with Security…

or Security works above HR..

..Check if top management is committed before you proceed..

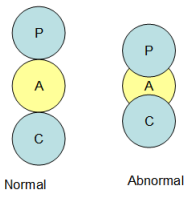
Deviant Behaviour identification and Correction

- There are several theories on deviant behaviour
  - Which can be customized to the corporate needs
  - To identify potentially risky employees
  - To develop appropriate tests for generation of early warning

Mapping of Employees..

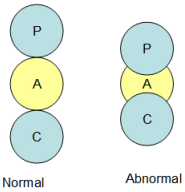
..Behavioural Science based strategies

EgoGram Approach



- Based on Eric Berne's TA theory
- Develop Egogram maps for every employee
  - As a byproduct of training for "Organizational Effectiveness" or "Leadership"

EgoGram Approach



- Every individual is a bundle of behavioural patterns
  - Rules of life imbibed in eary age
  - Rational behaviour
  - Emotional behaviour
- A deviant mind reflects less of rational behaviour

Develop egograms for every employee ..As a byproduct of training for "Organizational Effectiveness" or "Leadership"

Script Mapping

Dr Thomas Harris

I am Not OK You're OK	I am Not OK, You're Not OK
I am OK, You're OK	I am OK, You are not OK

Every person develops a "Script" based on his experiences and his behaviour is influenced by such scripting.

A criminal is more likely to have a "I am Not OK, You are Not OK" script

A typical terrorist is likely to have a "I am OK, You are Not OK" script

Develop Script maps for every employee ..As a byproduct of training for "Organizational Effectiveness" or "Leadership"

Data Mining

- Intelligence gathering through
  - Social networking Sites,
  - Blogs,
  - E Mails,
  - Honeypots
- NLP (Natural Language Processing)
  - Analysis of text based artefacts
- Artificial Intelligence in CCTV analysis
  - A Comprehensive Strategy Required to classify the risk propensity of employees

Corrective Programme

- Basic approach for all
  - Senitization through awareness training
  - Ethical Declaration.. To get personal commitment
- Core Employee Risk Sanitization Programme
  - For the shortlisted persons based on classification, observation, egogram and script mapping
    - Leadership quality enhancement Programmes
    - Team Player Attribute enhancement Programmes
    - Self improvement through hypnotic suggestive techniques

Whistleblowing

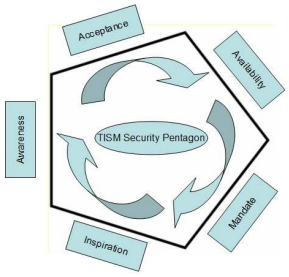
- A key ingredient to any Security Policy involving people
  - Requires an appropriate system independent of the insider control
    - Ombudsman who receives and filters complaints, de-identifies the whistleblower and then initiates action at the CSO level
    - Assures witness protection if not reward
- Check out "CEAC-Ombudsman"

Theory of IS Motivation

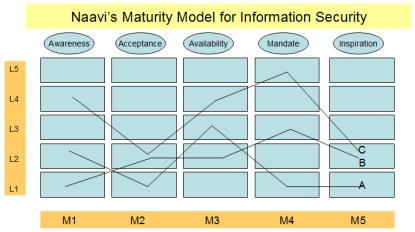
Security Adoption is not a factor of Availability of Security Products

Employees must be aware of the need for security and accept it.

Must be supplemented with a mandate and use of inspired champions



Assess Organizatons based



Next Step

- Champion the PIH Approach to Security in your organization
  - Integrate HR and IS Policies with overall Organizational Security policies
- Review the "Background Check" policy for employee recruitment
- Initiate discussion with the training division
  - For 100% employee sensitization on security
- Initiate or Review Whistle Blower Policy
- Initiate action for mapping the security threats in employees in consultation with experts who understand Security and Behavioural Science
  - Mitigation strategies may be taken up later

Thank you

- Contact
  - naavi@vsnl.com
  - 9343554943
- www.naavi.org
- www.cyberlaws4cxo.com