Lessons Learnt for Security Crisis Management

Patrick Nathan

SMRT, Director Security Operations And Readiness, Singapore

2013 Rail Conference

Key Lessons Learnt

1. Understand the Security Environment, KPIs and Mission
2. Develop a Security Management Framework
3. Undertake the Security Repairs
4. Putting in place Crisis Management and Emergency Response Structures
5. Defining clearly their Roles
6. Being clear about the Activation process
7. Identifying Key Decisions and Timelines
8. Setting up Crisis Management and Emergency Response Rooms
9. Developing an Integrated Emergency Management Plan
10. Putting together a Workplan: SOP Reviews, Briefings and Exercises
11. Alignment of Alert Levels and Synchronization of SOPs
12. Criticality of first half hour: Engaging the public early

1. Understand the Security Environment

- Close to a hundred stations
- Many miles of above ground/at grade tracks
- Close to 20 SMRT facilities like depots, interchanges, HQ and Operational Control Centres
- Many facilities are classified National Critical Infrastructure
- SMRT is an Essential Firm
- Public transport networks: vulnerable and attractive targets

1. Understand the Security KPIs

- Code of practice governing security in the MRT system: 22 reqts
- Code of practice governing security in the LRT and Bus system: another 23 reqts
- 2-monthly internal audits and yearly external audits
- Security audits on stations and red teaming exercises on depots
- Security KRI reporting to Management Comm and Board: 9 items

1. Understand the Security Mission

- Zero security incidents
- Security officers are at their post and conduct their patrols
- Security officers are not depending on Technology to be alerted to intrusions
- Intrusions if they do occur are reported quickly
- Overlapping security processes work. This means two things
  - Intrusion detection and mitigation
  - Checks on operations and infrastructure
- Passing all external and internal audits and checks

2. Develop a Security Management Framework

Framework

- Assess
- Prevent
- Protect
- Respond
- Recover

Processes

Risk Assessment
Risk Events:
External Threats, SMRT-wide Risks and Business Unit Risks
Risk Analysis:
Top Risks & Emerging Risks, Key Risk Indicators and Risk Reporting

Risk Management
Security Hardware:
Security Improvement Plan
Security Manpower:
Security Officers, SMRT Staff, Premises Managers, Front-line Staff, Red Teamers and BCM Coordinators
Security Practices:
Code of Practice, Perimeter Patrols, Exterior checks of Trains and Security Screening
Security Culture:
Security Tagline, Appraisal System and Internal Audit
Security Training:
Threat Mitigation and Protocols
Security Agenda:
Security Exercises, Audits and Programmes

Crisis Management
Crisis Events:
Internal, External and National
Crisis Response:
Incident Management Plans and Crisis Management Teams

3. Undertake the Security Repairs

- Strengthening the core security team
- Reviewing SOPs
- Reviewing patrol routes and patrol routines
- Improving monitoring
- Putting the right security infrastructure in place quickly
- Clearing up security ownership issues
  - Linked to the more difficult issue of culture
- Putting in additional layers of defence

3. Undertake the Security Repairs

- One vs. Two service providers
- Short term vs. Long term partnership
  - Better technology and infrastructure amortized over a longer period
- High-end industry-leading specifications
  - Training and competence
  - Management structure e.g. OEs and OMs
  - Dedicated Operations Centre
  - High LD as guarantee of service
  - Flexible LD structure for smooth induction reducing to zero infringements over one year
  - Mandatory 2 off days per week
- Transparent over job description and SOPs

4. Putting in place Crisis Management and Emergency Response Structures

- Principles:
  - Separate the Strategic, Operational and Tactical Layers (Gold, Silver and Bronze)
    - Crisis Management Team
    - Emergency Response Team
    - Operations Control Centre
  - Have the essential functional responsibilities represented in your teams
  - Appoint Primary and Alternate members
    - Routine: Overseas leave/duty
    - Prolonged disruptions: Team A/Team B
    - Pandemics: Split Team operations
  - Managing Multiple Incidents

5. Defining clearly their Roles

- Principles:
  - As a member of the team and individually as a Key Appt Holder
  - Statutory duties should be clearly highlighted

6. Being clear about the Activation Process

- Principles:
  - Top down and bottom up processes
  - What is done at each level
  - Simple flowchart

7. Identifying Key Decisions and Timelines

- Principles:
  - Useful aide memoire for Crisis Managers in a crisis
  - Constant reminder to make/defer decisions by a certain time
  - Based on experiences in past crises
  - Secretariat to administer this and record key decisions
    - Facilitates the After Action Review
  - Shows critical dependencies

8. Setting up Crisis Management and Emergency Response Rooms

- Principles:
  - – Keep the strategic, operational and tactical teams separate
    - Avoids a trading floor environment
    - Reduces temptation to interfere
  - – Give them each the comms, situation awareness pictures and aide memoires they need

9. Developing an Integrated Emergency Management Plan

- Principles:
  - Importance of having an Integrated Emergency Management Plan
    - Integrating it into your Enterprise Risk Management framework
    - Critical Interdependencies are clearer
  - Develop SOPs only where you need them

10. Putting together a Workplan: SOP Reviews, Briefings and Exercises

- Principles:
  - Annual and periodic reviews of SOPs
    - Especially after an incident has occurred
  - Annual and periodic briefings of SOPs
    - Especially when there is a large turn-over in staff
  - Annual exercises
    - Component level exercises
    - Scenario based exercises
    - Table Top and Ground Deployment exercises
  - Seasonal and staggered

11. Alignment of Alert Levels and Synchronization of SOPs

- Principles:
  - We need to be sure we have the same understanding/use the same language as the emergency services/regulator
    - Critical when you need to depend on external agencies
    - Especially when there are far-reaching implications for e.g. shutdown of the transport network
  - We need to be clear about the roles of Incident Manager and Crisis Manager
    - Who does what, when/handover and takeover points

12. Criticality of first Half Hour: Engaging the public early

- Principles:
  - The public transport "war" is won or lost in the first half hour
  - Applies to
    - Public communications
    - More staff on the ground (security situation permitting)
    - Bus bridging when train service is disrupted (security situation permitting)
  - Importance reflected in Code of Practice

Summary

1. Understand the Security Environment, KPIs and Mission
2. Develop a Security Management Framework
3. Undertake the Security Repairs
4. Putting in place Crisis Management and Emergency Response Structures
5. Defining clearly their Roles
6. Being clear about the Activation process
7. Identifying Key Decisions and Timelines
8. Setting up Crisis Management and Emergency Response Rooms
9. Developing an Integrated Emergency Management Plan
10. Putting together a Workplan: SOP Reviews, Briefings and Exercises
11. Alignment of Alert Levels and Synchronization of SOPs
12. Criticality of first half hour: Engaging the public early

Final words

- Evolving Emergency Planning to Emergency Preparedness to Operational Readiness:
  - Investing in more and better EP and Security resources
  - Adding the Audit and Operational Readiness functions
  - Emphasis on anticipation (PPRR cycle)
- Ministry, Stat Boards and Operators must work together
  - Put in place integrated EP and Security framework, structures and processes
  - Consistently apply risk management approach
  - Consistently apply "are policies implementable?" approach
  - Establishing and publishing clear and implementable standards
  - Removing onerous administrative layers

Thank You

Patrick Nathan

Director, Security Operations
And Readiness

PatrickN@smrt.com.sg