Enterprise Incident Management @ SSHA

Bobby Singh

Director – Information Security

Smart Systems for Health Agency

Ontario
Smart Systems for Health Agency

Agenda

- SSHA Mandate
- Approach & Deliverables
- Lessons Learned
- Measurement

SSHA: Transforming Healthcare through IT

- Providing healthcare providers with timely, secure electronic access to patient information
- Creating a secure patient information sharing network between 150,000 providers at 24,000 sites
- The results:
  - Improved patient care
  - More effective providers
  - Integration
  - Better use of financial resources

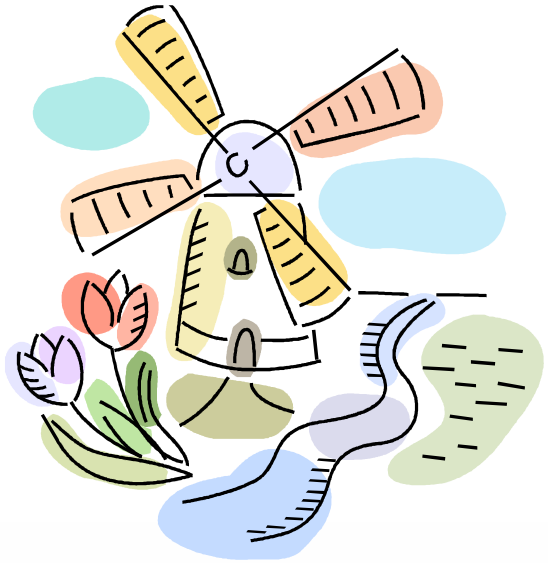
Who is SSHA connecting?

- Doctors
- Hospitals
- Pharmacists
- Laboratories
- Public Health Units
- Community care
- Continuing care
- Ministry of Health and Long-Term Care programs

Program Objectives and Scope

- A single program to manage *Privacy and Security* incidents
- The scope of the ESPIM (Enterprise Security & Privacy Incident Management Program) program is limited to incident management, as it pertains to security or privacy incidents that meet a particular threshold or severity. IT/Network service incident management, incident monitoring and problem management are outside of the mandate of the program

Strategy – IOC & FOC



Initial Assessment – example

Maturity Level		IM Technical Capability					IM Operational Capability		
Scale		Threat monitoring	Security monitoring tools	Vulnerability management	Configuration management	Forensics / Log management	Incident handling	Coordination (IPC/SOC)	Knowledge Management
Highest	5 - efficient	By invite only	Apps / host / OS monitoring	Integrated patch management system	Enterprise Automated config monitoring	HR/Legal forensics collection	Communications planning, coordination and distribution	Enterprise integrated governance structure	Predicative analysis
	5 - optimised	Active association participation	System device	EVA with threat correction	Enterprise CMDB		Monitoring and logging standard	Integrated IPC/SOC - internal response capabilities	Detailed trend analysis
	4 - managed and measurable	FIRST membership	Security event monitoring	EVA	CMO/CMM board	Digital forensics collection	Evidence collection policy Regular IH testing	Internal advisory support Mature IH	Data mining
		Commercial feed / ITAC	HIDS		Problem management	Centralised log management	Monitoring policy	Integrated toolkit architecture	Reporting portal
	3 - defined processes		Security sensors	Scheduled VA			Integrated process	Mid IH and Security monitoring	Consolidated reporting
	2 - repeatable but intuitive	RSS feeds	Security devices	Ad hoc VA	Help Desk	Co-ordinated logging	Generic process	Concept of operations / Strategy / Charter vision	Tool generated reports
	1 - initial ad hoc	Ad hoc browsing	Manual log reviews	Ad hoc patching	Ad hoc system CM process	Ad hoc logging	NAUP		
Lowest	0 - non existent	None	None	As Noticed	None	None	Ad hoc	None	None

FIRST Improving Security Together
2008 SPEAKER

Initial Assessment – example

Maturity Level		IM Technical Capability					IM Operational Capability		
Scale		Threat monitoring	Security monitoring tools	Vulnerability management	Configuration management	Forensics / Log management	Incident handling	Coordination (IPC/SOC)	Knowledge Management
Highest	5 - efficient	By invite only	Apps / host / OS monitoring	Integrated patch management system	Enterprise Automated config monitoring	HR/Legal forensics collection	Communications planning, coordination and distribution	Enterprise integrated governance structure	Predicative analysis
	5 - optimised	Active association participation	System device	EVA with threat correction	Enterprise CMDB		Monitoring and logging standard	Integrated IPC/SOC - internal response capabilities	Detailed trend analysis
	4 - managed and measurable	FIRST membership	Security event monitoring	EVA	CMO/CMM board	Digital forensics collection	Evidence collection policy Regular IH testing	Internal advisory support Mature IH	Data mining
		Commercial feed / ITAC	HIDS		Problem management	Centralised log management	Monitoring policy	Integrated toolkit architecture	Reporting portal
	3 - defined processes		Security sensors	Scheduled VA			Integrated process	Mid IH and Security monitoring	Consolidated reporting
	2 - repeatable but intuitive	RSS feeds	Security devices	Ad hoc VA	Help Desk	Co-ordinated logging	Generic process	Concept of operations / Strategy / Charter vision	Tool generated reports
	1 - initial ad hoc	Ad hoc browsing	Manual log reviews	Ad hoc patching	Ad hoc system CM process	Ad hoc logging	NAUP		
Lowest	0 - non existent	None	None	As Noticed	None	None	Ad hoc	None	None

FIRST Improving Security Together
2008 SPEAKER

Initial Assessment – example

Maturity Level		IM Technical Capability					IM Operational Capability		
Scale		Threat monitoring	Security monitoring tools	Vulnerability management	Configuration management	Forensics / Log management	Incident handling	Coordination (IPC/SOC)	Knowledge Management
Highest	5 - efficient	By invite only	Apps / host / OS monitoring	Integrated patch management system	Enterprise Automated config monitoring	HR/Legal forensics collection	Communications planning, coordination and distribution	Enterprise integrated governance structure	Predicative analysis
	5 - optimised	Active association participation	System device	EVA with threat correction	Enterprise CMDB		Monitoring and logging standard	Integrated IPC/SOC - internal response capabilities	Detailed trend analysis
	4 - managed and measurable	FIRST membership	Security event monitoring	EVA	CMO/CMM board	Digital forensics collection	Evidence collection policy Regular IH testing	Internal advisory support Mature IH	Data mining
		Commercial feed / ITAC	HIDS		Problem management	Centralised log management	Monitoring policy	Integrated toolkit architecture	Reporting portal
	3 - defined processes		Security sensors	Scheduled VA			Integrated process	Mid IH and Security monitoring	Consolidated reporting
	2 - repeatable but intuitive	RSS feeds	Security devices	Ad hoc VA	Help Desk	Co-ordinated logging	Generic process	Concept of operations / Strategy / Charter vision	Tool generated reports
	1 - initial ad hoc	Ad hoc browsing	Manual log reviews	Ad hoc patching	Ad hoc system CM process	Ad hoc logging	NAUP		
Lowest	0 - non existent	None	None	As Noticed	None	None	Ad hoc	None	None

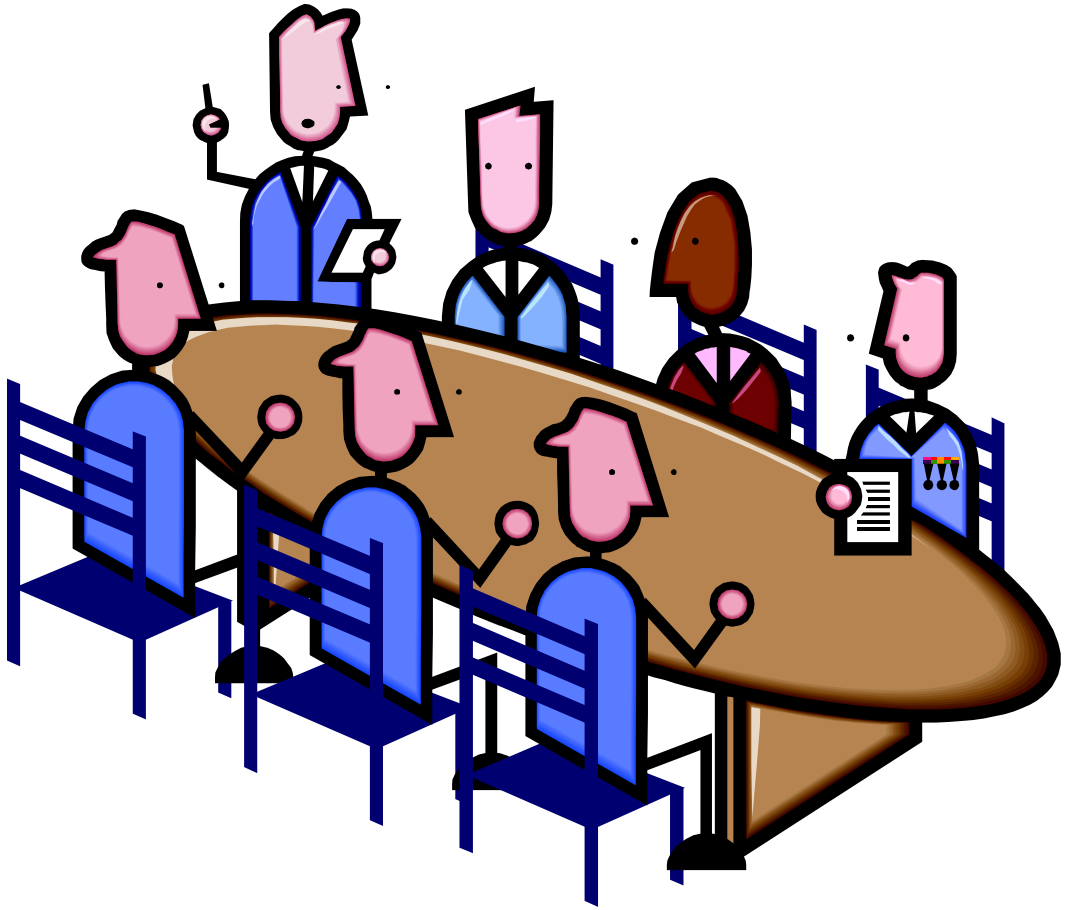
FIRST Improving Security Together 2008 SPEAKER

Initial Assessment – example

Maturity Level		IM Technical Capability					IM Operational Capability		
Scale		Threat monitoring	Security monitoring tools	Vulnerability management	Configuration management	Forensics / Log management	Incident handling	Coordination (IPC/SOC)	Knowledge Management
Highest	5 - efficient	By invite only	Apps / host / OS monitoring	Integrated patch management system	Enterprise Automated config monitoring	HR/Legal forensics collection	Communications planning, coordination and distribution	Enterprise integrated governance structure	Predicative analysis
	5 - optimised	Active association participation	System device Security event monitoring	EVA with threat correction	Enterprise CMDB		Monitoring and logging standard	Integrated IPC/SOC - internal response capabilities	Detailed trend analysis
	4 - managed and measurable	FIRST membership		EVA	CMO/CMM board	Digital forensics collection	Evidence collection policy Regular IH testing	Internal advisory support Mature IH	Data mining
		Commercial feed / ITAC	HIDS		Problem management	Centralised log management	Monitoring policy	Integrated toolkit architecture	Reporting portal
	3 - defined processes		Security sensors	Scheduled VA			Integrated process	Mid IH and Security monitoring	Consolidated reporting
	2 - repeatable but intuitive	RSS feeds	Security devices	Ad hoc VA	Help Desk	Co-ordinated logging	Generic process	Concept of operations / Strategy / Charter vision	Tool generated reports
	1 - initial ad hoc	Ad hoc browsing	Manual log reviews	Ad hoc patching	Ad hoc system CM process	Ad hoc logging	NAUP		
Lowest	0 - non existent	None	None	As Noticed	None	None	Ad hoc	None	None

FIRST Improving Security Together 2008 SPEAKER

Strategy – joint application development (JAD) sessions



Joint Application Development (JAD) sessions

- 2 day session included members from
  - Communications (internal/external)
  - Security Operations
  - Human Resources
  - Change Management
  - Network Operations
  - Legal Department
  - Service Management
  - Business/Client Relationship Department
  - Customer/Help Desk Support
  - Privacy and Security Division
- 20 issues identified & 21 decisions documented

This formed the foundation for building ESPIM

Key Terms defined:

- Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.
- Service Incident: Any contact pertaining to service interruptions, inquiries, issues, complaints, and service.
- Security Incident: A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- Privacy Incident: Unauthorized or illegal use, collection, disclosure, or disposal of personal or personal health information. Until confirmed to be real, it is classified as an incident.
- Privacy Breach: A Privacy incident where it has been confirmed that unauthorized or illegal use, collection, disclosure, or disposal of personal or personal health information has occurred.
- ESPIM Incident: A Security or Privacy Incident that meets the ESPIM criteria thresholds.

ESPIM Triggering Thresholds

- Not every security or privacy incident is automatically considered an ESPIM incident.
- For a security or privacy incident to trigger an ESPIM incident, the following thresholds must be met -

ESPIM Incident Type	Severity to Trigger
Malware	High
Network Attack	Medium
Privacy Breach	Medium
Unauthorized Use	All
Missing Equipment	Internal – High Client - All

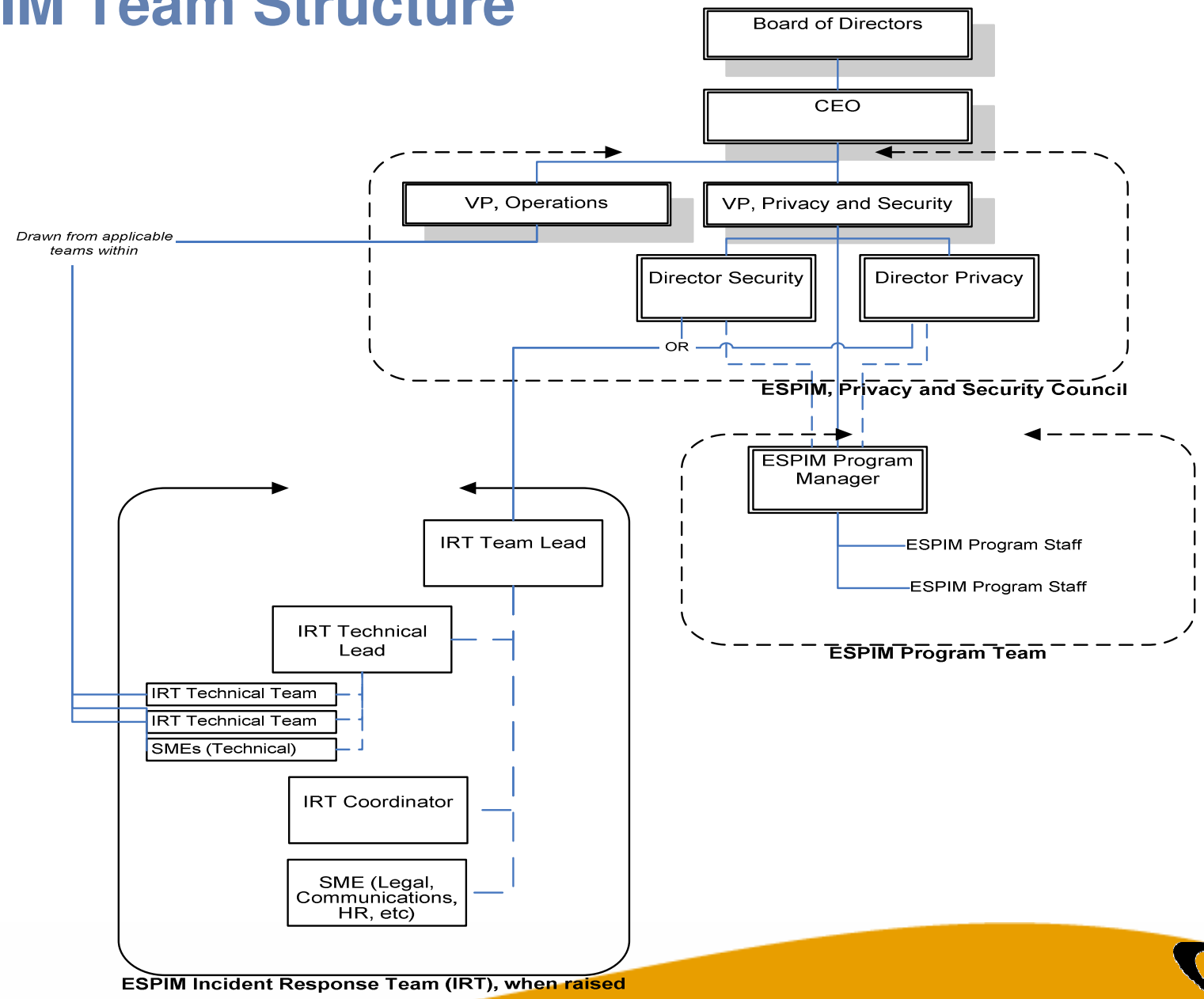
The end-point program - ESPIM thresholds

Type	Item	Escalation threshold to ESPIM
Account Compromise	User/Administrator/Other	A system or data is accessed by an unauthorized person
Denial of Service	User System	Problem affecting 2 or more users
Malicious Code	Virus/Trojan Horse/Other	Problem affecting 2 or more users
Lost or stolen asset	Blackberry /Security Badge	Evidence that it is being used by an unauthorized user
Lost or stolen asset	Computer/Printed Documentation/Storage Media/Electronic Data/Other	Possibly containing PI/PHI, not encrypted, or used by an unauthorized user
Privacy Incidents	Unauthorized Collection / Use / Disclosure / Disposal	Any and all privacy incidents are priority 2 by default

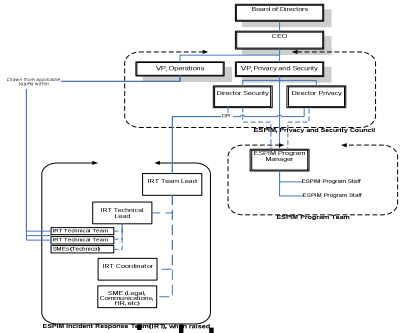
Incident Examples

Incident Types	Example	ESPIM Threshold
Unauthorized Access	Someone discovers user password or shares it	Only if password used to access system by unauthorized individual
Unauthorized Use	Unauthorized use of network resources for spam mail	Only if spam mail affects availability of services and malicious content
Unauthorized Collection	Collection of server configuration (Collection of PHI data)	Only if configuration used to change system settings or affect service
Lost Asset	Employee blackberry lost/stolen	Only if used by unauthorized person or contain PHI data
Unauthorized Disclosure	PHI data disclosed publicly	Any scenario
Unauthorized Disposal	PHI data not retained on-line and could not be restored from backup	Any PHI data not available for use meet privacy incident
Denial of Service	User unable to access applications on their workstation	Only if it impacts two (2) or more users
Malware	User opens e-mail attachment with virus	Only if it impacts two (2) or more users

ESPIM Team Structure



ESPIM Composition



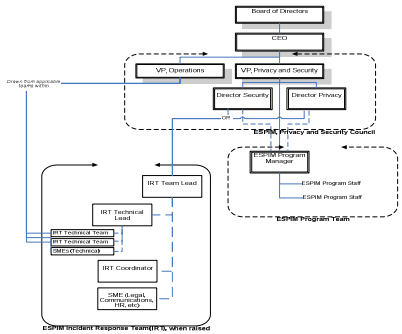
The ESPIM Program is composed of three primary groups:

- **ESPIM Oversight Committee**: Management control and oversight of the ESPIM program, along with provision of interdepartmental alignment of activities will be performed by an ESPIM Oversight Committee.
- **ESPIM Program Team**: A permanent team, responsible for the day to day operations of the ESPIM Program.
- **ESPIM Incident Response Team**: A dynamically assigned team, raised to handle individual ESPIM incidents.

ESPIM Roles and Responsibilities: *ESPIM Program*

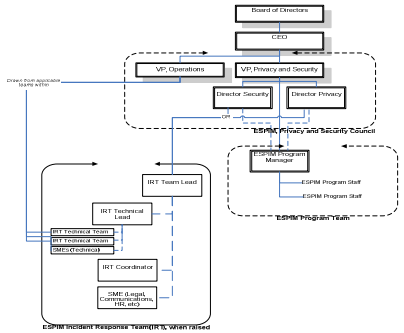
- **ESPIM Program Manager**: is responsible for ensuring that ESPIM services are provided including the day-to-day activities of the ESPIM Program, up to but not including specific incident handling.

- **ESPIM Incident Response Team (IRT) Lead**: Drawn from the ESPIM Program team, the Security department, or the Privacy department, is responsible for:
  - logistical co-ordination of the IRT, both within the team and between the team and others,
  - incident communications, and
  - post-incident analysis activities.



ESPIM Roles and Responsibilities: *ESPIM IRT Technical Team*

- **ESPIM IRT Technical Team Lead**: Drawn from the Operations department, or an external SME. Is responsible for:
  - leads the technical response for incident;
  - works closely with the IRT Lead and the IRT Technical Team Lead;
  - performs incident identification and analysis;
  - determine containment and eradication solution strategies; and
  - determining a solution deployment strategy.



Key ESPIM Documentation

- ESPIM Strategy: outlines the approach taken to implement the Best Practices Model and the Business Requirements, and describes the operational and technical issues and challenges that will be faced by the ESPIM Program.
- ESPIM Concept of Operations: summarizes the operational model of the ESPIM Program, including the roles necessary to support the program, and the structure and reporting of the program.
- ESPIM Operating Directives: outline the acceptable ESPIM-related practices.
- ESPIM Communications Plan: describes the ESPIM-related communications (notifications, reporting, alerting, and informational notices) that will need to performed, along with guidance on who and how those communications are to be conducted.
- ESPIM Incident Handling Procedures: describes the specific steps to the be taken by the ESPIM IRT during incident handling.

Measurement (examples)

Quantitative Metrics:

- Mean time to initiate response to incidents by category
- Mean time to complete response to incidents by category
- Number of incidents that required external reporting or notification
- Trend reporting on incident resolution time, by incident type and severity levels
- Trend reporting on time to close post-incident analysis action items, by activity custody holder
- Statistical reporting of number of incidents handled, by incident type and severity levels
- Statistical reporting on % of incidents requiring external notifications
- Statistical reporting of number of alerts and advisories issued, by type

Qualitative Metrics:

- Summary of incidents handled
- Collective summary of lessons learned
- Client level of satisfaction with incident handling
- Reporting on business impacts of incidents, including losses (and costs where possible)

Key components

- Management Support
- Requirements/Needs Analysis
- Table Top Exercise
- Test the Communication Plan
- Test/Use Cases specifically for the program
- Checklist/Quick Reference Guide

ESPIM – Lessons learned

- JAD sessions ensured buy-in from most stakeholders. Identifying issues and decisions made early in the development process helped avoid misunderstanding
- Integrated but distributed approach ensured appropriate skills are available to the IRT when needed
- Defining IOC and FOC helped limit scope. This was made possible by the CMMi chart
- Table top exercise highlighted weaknesses in process / people that were subsequently fixed
- Separating program development from implementation allowed enough time for successful implementation
- Development, deployment and training in separate Privacy and Security use cases for help desk ensured ESPIM was embedded

Discussion / Questions

Contact Info:

Bobby Singh

416.586.4231

Bobby.singh@ssha.on.ca