Trusted By Design Inc.

"Creating Trust For Business"

BSides 2017

Risk-Based Security Incident Response (SIR) and An Introduction to SICON

Keith Jonah
CISSP, CISM, CRISC
kjonah@trustedbydesign.ca
416.727.3809

Kevin Pietersma
CISSP, SANS GCIA Gold
@bydasein
647.284.5387

Warning!

We are not here to explain the Security Incident Response process

But we do have a great SIR presentation for next year ;-)

Risk-based Decisioning in Security Incident (SI) Response (SIR)

- Concept of “risk decisioning during security incident handling”
- Input, quantifiable measures of impact and the degree of compromise at a point in time
  - Potential Impact (as set by the Business Unit)
  - Current Impact (in situ assessment)
  - SI Condition (SICON), the degree of compromise
- Output, “SI Severity Level” represents risk and is used to
  - Select a level of response
  - Determine the notification addressees and schedule of updates
  - Set the required seniority of assigned SIRT members

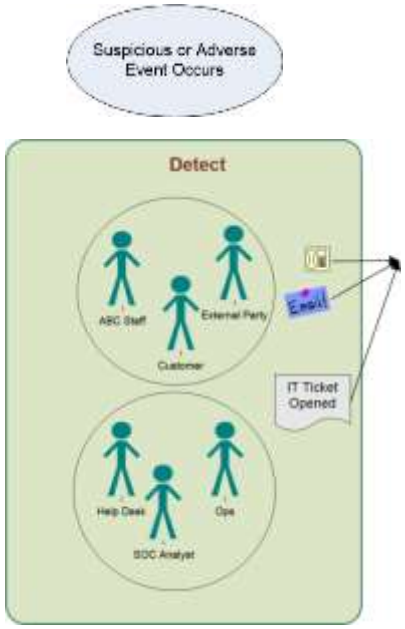
Things to Take Away

- Make decisions based on Impact, not just the Attack Vector. Like doing a live Threat & Risk Assessment (TRA)!
- SICON – your “at the moment” Security Incident CONdition of compromise
- SI Severity Levels standardizes way of appropriately handling Sis caused by any threat type
- Triage determines level of priority through SIR
- Using “non-linear starts” and iterations of assessment/response
- Use separate and secure Security Incident Ticket
- Some security incidents have nothing to do with eradication or containment… (lost laptop)… Kev’s pet peeve

Definitions

Adverse Event	Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
IT Incident	An IT incident is "an interruption to, or a reduction in the quality of an IT Service and requires intervention by IT Operations to restore." Adopted from the ABC Incident and Problem Management Process.
Security Incident (SI)	A computer Security Incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Note, the occurrence of a Security Incident does not necessarily mean that a malicious attack has been successful.
Malicious Attack	Deliberate and possibly ongoing attempts to circumvent security controls. Note, the occurrence of a Malicious Attack does not necessarily mean that it is or will be successful.
Security Incident Condition (SICON)	The "Security Incident Condition" (SICON), is the degree of compromise for a validated Security Incident as established by the SIRT upon assessment of the known circumstances at a point-in-time. The SICON may be revised by the SIRT as required as, typically based upon new information or new analysis during the Response and Eradicate & Recover Phases.
SI Severity Level	The priority with which a Security Incident (or Breach) should be handled is represented by its Severity Level. The SI Severity Level triggers the appropriate: • assignment of experienced personnel; • involvement of ABC Shared Services; • notification periods and distribution lists; • escalations of decision making to more senior ABC stakeholders
Imminent Threat of Violation	Refers to a situation in which the organization has a factual basis for believing that a specific Security Incident is about to occur.
Security Breach	A confirmed compromise of ABC service or information assets due to unauthorized disclosure, unauthorized modification/addition/deletion, or malicious disruption.
Material Security Breach	A confirmed compromise of ABC service or information assets with an Impact of HIGH or VERY HIGH due to unauthorized disclosure, unauthorized modification/addition/deletion, or malicious disruption.

Security Incident Response Framework



Validate

Triage

Mobilize

Intake

Respond

Security Incident Response Team (SIRT)

&

Shared Services

Iterative

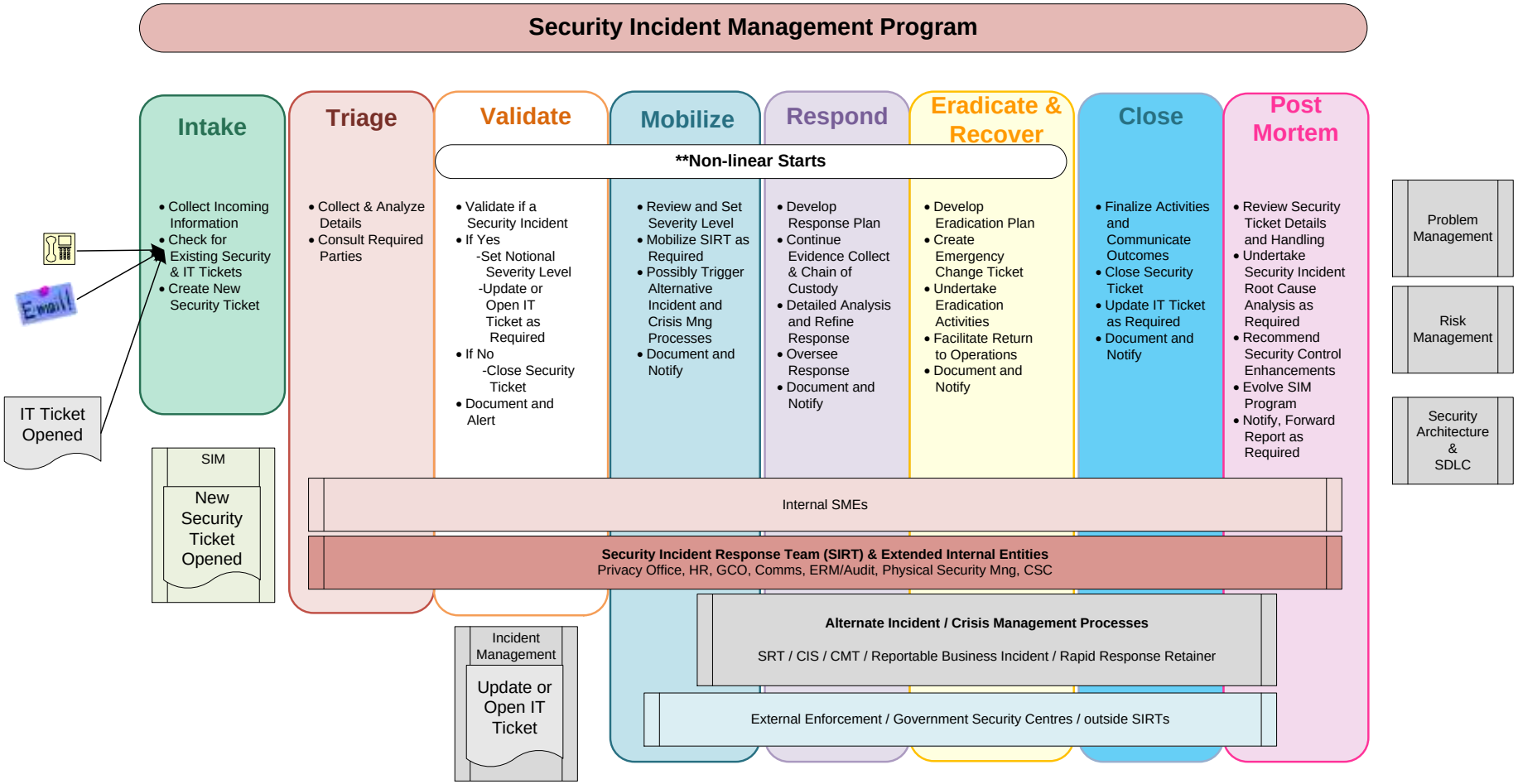
Eradicate & Recover

Evolve SIR

Post Mortem

Close

Non Linear Starts


Security Incident Management Program
Intake
• Collect Incoming Information
• Check for Existing Security & IT Tickets
• Create New Security Ticket
Triage
• Collect & Analyze Details
• Consult Required Parties
Validate
• Validate if a Security Incident
• If Yes
-Set Notional Severity Level
-Update or Open IT Ticket as Required
• If No
-Close Security Ticket
• Document and Alert
Mobilize
• Review and Set Severity Level
• Mobilize SIRT as Required
• Possibly Trigger Alternative Incident and Crisis Mng Processes
• Document and Notify
Respond
• Develop Response Plan
• Continue Evidence Collect & Chain of Custody
• Detailed Analysis and Refine Response
• Oversee Response
• Document and Notify
Eradicate & Recover
• Develop Eradication Plan
• Create Emergency Change Ticket
• Undertake Eradication Activities
• Facilitate Return to Operations
• Document and Notify
Close
• Finalize Activities and Communicate Outcomes
• Close Security Ticket
• Update IT Ticket as Required
• Document and Notify
Post Mortem
• Review Security Ticket Details and Handling
• Undertake Security Incident Root Cause Analysis as Required
• Recommend Security Control Enhancements
• Evolve SIM Program
• Notify, Forward Report as Required
**Non-linear Starts
Problem Management
Risk Management
Security Architecture & SDLC
IT Ticket Opened
SIM
New Security Ticket Opened
Incident Management
Update or Open IT Ticket
Internal SMEs
Security Incident Response Team (SIRT) & Extended Internal Entities
Privacy Office, HR, GCO, Comms, ERM/Audit, Physical Security Mng, CSC
Alternate Incident / Crisis Management Processes
SRT / CIS / CMT / Reportable Business Incident / Rapid Response Retainer
External Enforcement / Government Security Centres / outside SIRTs

Supporting Risk Exercises

In due course, prior to the Security Incident:

- Enterprise develops their Impact Rating table
- Business Continuity/ Disaster Recover Planning undertake Business Impact Assessments (BIA) to establish “Potential Impact”
- Threat & Risk Assessments (TRAs) also can establish “Potential Impact” (amongst other things)
- Results roll up into a CMDB for assets, as well as Information Security Risk Repository for controls, vulnerabilities, threat agents, threat scenarios etc.

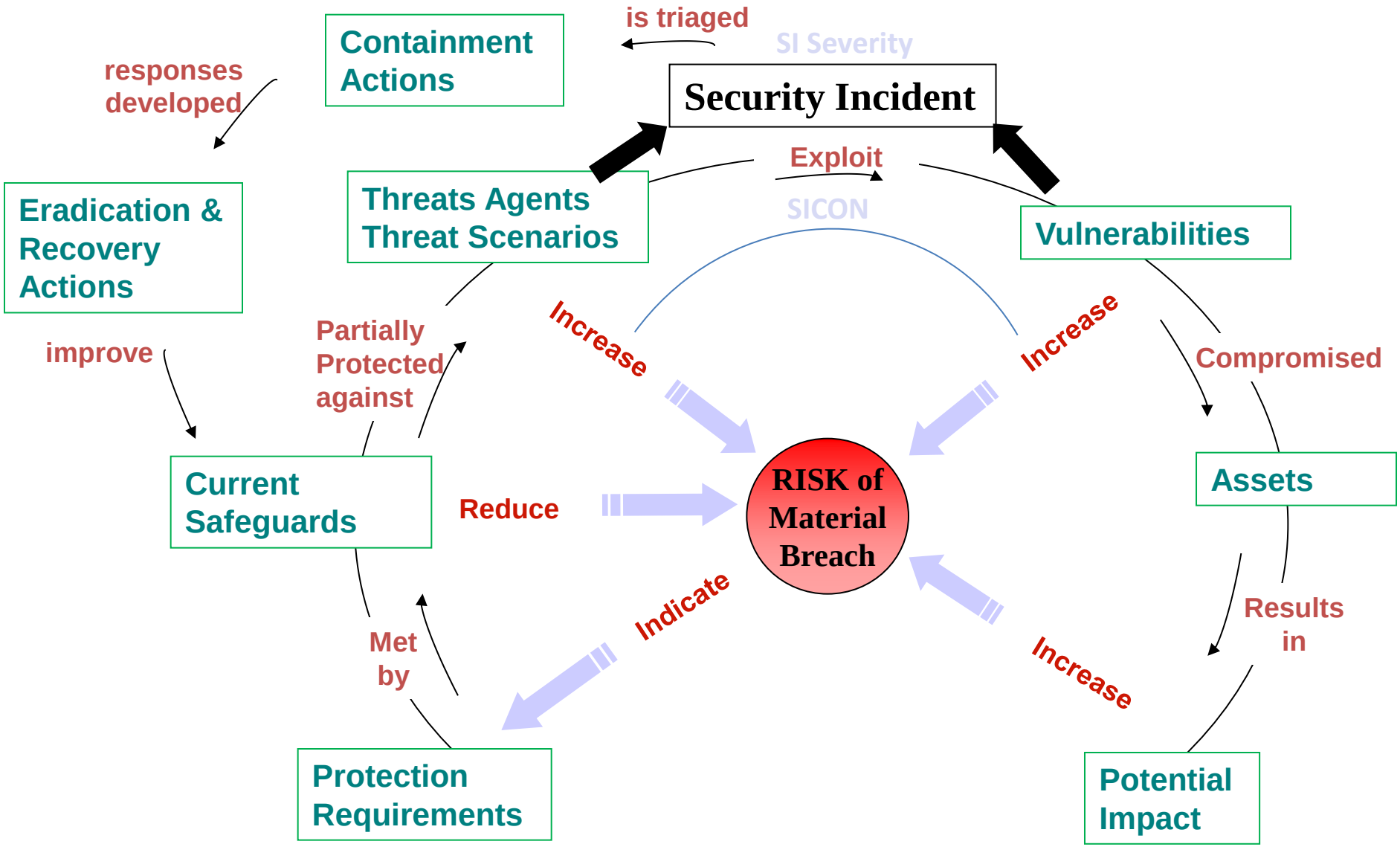
“Potential Impact” Rating Table

ERM Impact Levels as Applied to Potential (Assessed by BU Prior to an Incident) & Current (During a Security Incident)					
Impacat Rating	**Title**	**Financial**	**Reputation**	**Legal & Regulatory**	**Operational**
1	Very High	•Direct loss or cost of >50% of annual earnings •Credit rating downgrade to below "investment grade", meaning BB or B category; unable to raise full amount of required capital	•Adverse international media coverage •Major public concerns raised •Major loss of shareholder support •Loss of many key customers •Near unanimous criticism by opinion leaders; major government intervention is proposed	•Loss of license/s • Potential Litigation >$200 Million	•Large number of key executives/directors leaves company •Severe impact on the provision of critical services and recovery outside of acceptable recovery objectives •Work related death or serious injury of any individual •Operating loss including damage to third party property >$1 Million
2	High	•Direct loss or cost of 20-50% of annual earnings •Credit rating downgrade, but continue to be rated in BBB category or above	•Adverse national media coverage •Significant decrease in shareholder support •Loss of a key customer •Several opinion leaders suggest TMX Group is at fault; government intervention is suggested by some	•Regulator requires immediate press statement •Regulatory imposed fines •Potential Litigation $100 to $200 Million	•Some key executives leave the company •Severe impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $500K to $1 Million
3	Medium	•Direct loss or cost of up to 10-20% of annual earnings •Put on credit watch, but continue to be rated in A category or above	•Adverse local media coverage •Concerns raised by shareholders •Customers threaten to move business •Extended negative news coverage, with TMX Group described as being at fault	•Regulatory formal written warning •Potential Litigation $50 to $100 Million	•A key employee leaves •Significant impact on the provision of critical services and recovery outside of acceptable recovery objectives •Operating loss including damage to third party property in excess of $100K to $500K
4	Low	•Direct loss or cost of up to 5-10% of annual earnings	•Industry knowledge of incident, but no media attention •Client/Customer concerns •TMX is linked to negative news coverage, but is not the catalyst	•Verbal warnings from Regulators •Potential Litigation $10 to $50 Million	•Some staff morale problems •Significant impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $50K to $100K
5	Very Low	•Direct loss or cost of up to 1-5% of annual earnings	•Reputation intact, internal knowledge only •Minimal or no impact on customers •Letters containing negative sentiments sent to senior management and the Board	•Regulatory requirements not met •No reprimand or special undertaking •Potential Litigation between $1 and $10 Million	•Operating loss including damage to third party property <$50K •Some impact on the provision of critical services

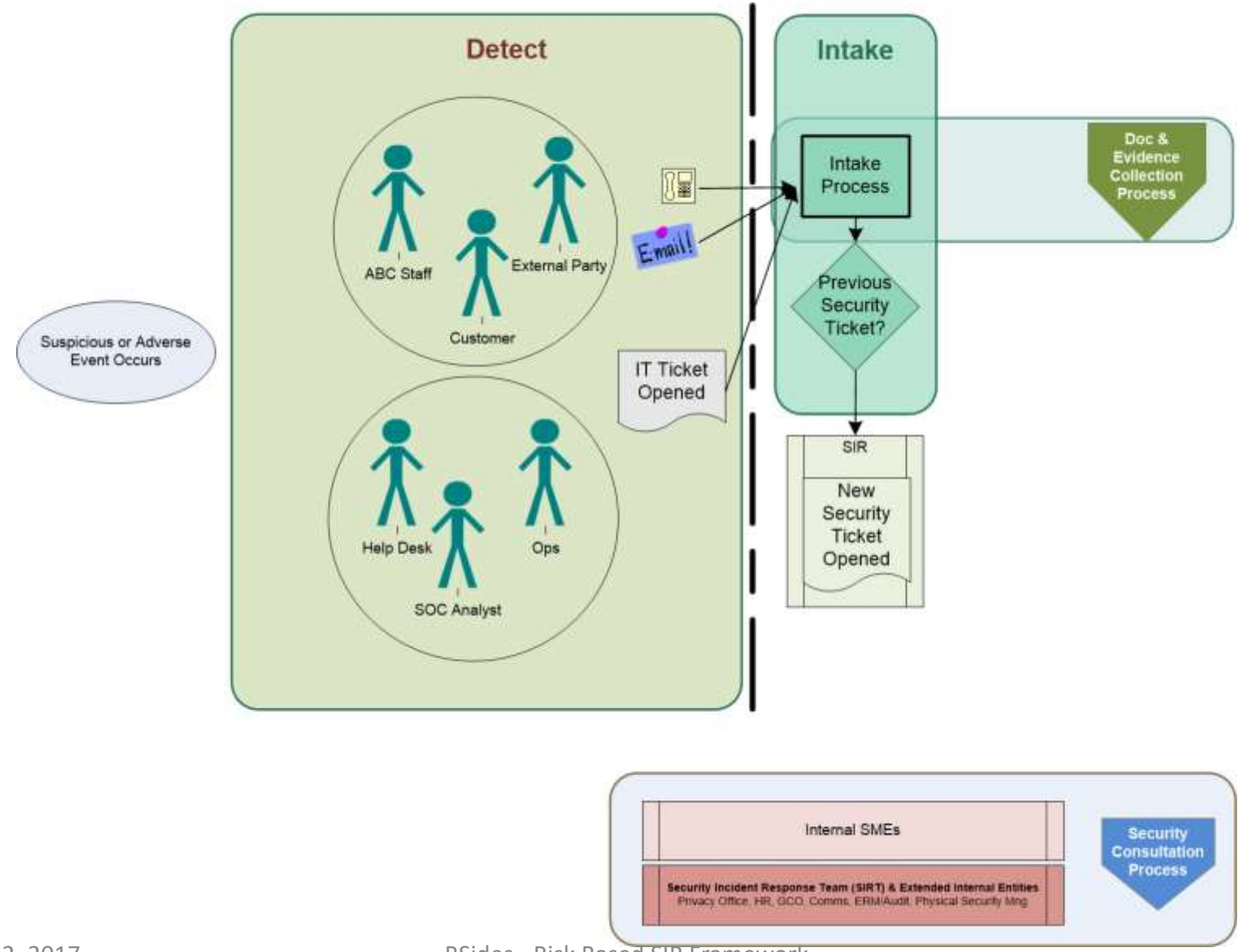
BU Critical IT Applications in CMDB

BU	Critical Application/System	Who supports this application? (ABC IT or vendor)	Most Sensitive Information Accessed or Transferred	Potential Impact (of Loss or Compromise)	RPO (Recover Point Objective)	RTO (Recovery Time Objective)	Confidentiality	Integrity	Availability	Personal	Regulated	Very High Availability
ABC-BU	***ABC-BU-SPECIFIC APPS.***											
	APP-1 (VENDOR-1)	Vendor	APP-1 files on ABC-BU NAS (Network Access Storage)	4-High	2 hours	NO loss of data	2	2	1			Y
	APP-2 (VENDOR-2)	Vendor	APP-2 files on ABC-BU NAS (I:\Drive)	4-High	2 hours	NO loss of data	2	1	1		Y	Y
	APP-3 (VENDOR-3)	Vendor	Member A/C info	3-Med	2 hours	NO loss of data	3	1	1			Y
	APP-4 (via Bloomberg)	Vendor	APP-4 Pricing file	2-Low	2 hours[2]	NO loss of data	2	1	1			Y
	CORPORATE INFRASTRUCTURE											
	Citrix Metaframe	ABC-IT	ABC-BU Application to access most critical applications/files	4-High	2 hours	NO loss of data	2	1	1			Y
	CISCO VPN	ABC-IT	ABC-BU staff username/password & ABC-BU IP addresses	3-Med	UNKNOWN	NO loss of data	2	1	1			Y
	MS Outlook (e-mail Archives, calendar…)	ABC-IT	.PST file for ABC-BU staff	2-Low	2 hours	4 hours	3	2	1		Y	
	Network Drives (I:\, J:\...)	ABC-IT	CRITICAL files (too many to enumerate)	4-High	2 hours	2 – 4 hours	2		1			Y

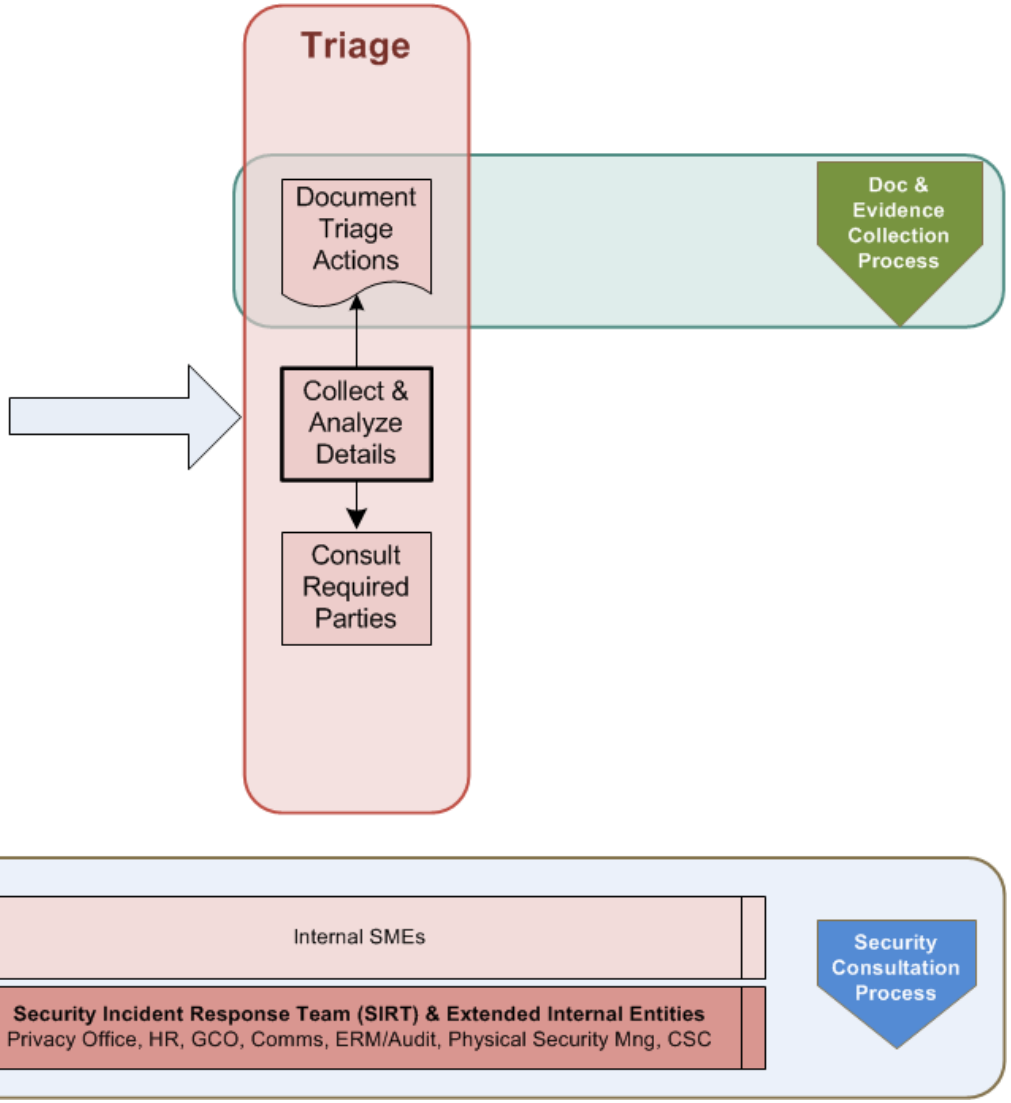
Security Risk & Security Incident / Breach Model



SIR Intake Phase



Triage Phase



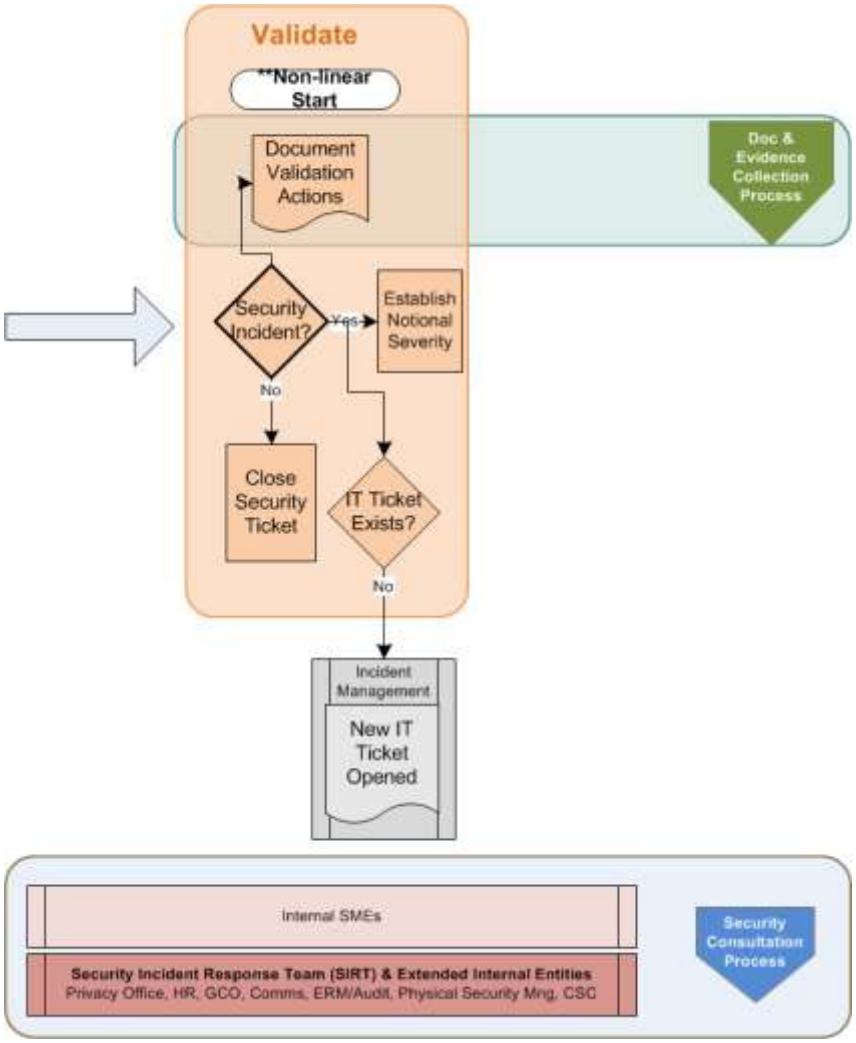
Current Impact

ERM Impact Levels as Applied to Potential (Assessed by BU Prior to an Incident) & Current (During a Security Incident)					
Impacat Rating	**Title**	**Financial**	**Reputation**	**Legal & Regulatory**	**Operational**
1	Very High	•Direct loss or cost of >50% of annual earnings •Credit rating downgrade to below "investment grade", meaning BB or B category; unable to raise full amount of required capital	•Adverse international media coverage •Major public concerns raised •Major loss of shareholder support •Loss of many key customers •Near unanimous criticism by opinion leaders; major government intervention is proposed	•Loss of license/s • Potential Litigation >$200 Million	•Large number of key executives/directors leaves company •Severe impact on the provision of critical services and recovery outside of acceptable recovery objectives •Work related death or serious injury of any individual •Operating loss including damage to third party property >$1 Million
2	High	•Direct loss or cost of 20-50% of annual earnings •Credit rating downgrade, but continue to be rated in BBB category or above	•Adverse national media coverage •Significant decrease in shareholder support •Loss of a key customer •Several opinion leaders suggest TMX Group is at fault; government intervention is suggested by some	•Regulator requires immediate press statement •Regulatory imposed fines •Potential Litigation $100 to $200 Million	•Some key executives leave the company •Severe impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $500K to $1 Million
3	Medium	•Direct loss or cost of up to 10-20% of annual earnings •Put on credit watch, but continue to be rated in A category or above	•Adverse local media coverage •Concerns raised by shareholders •Customers threaten to move business •Extended negative news coverage, with TMX Group described as being at fault	•Regulatory formal written warning •Potential Litigation $50 to $100 Million	•A key employee leaves •Significant impact on the provision of critical services and recovery outside of acceptable recovery objectives •Operating loss including damage to third party property in excess of $100K to $500K
4	Low	•Direct loss or cost of up to 5-10% of annual earnings	•Industry knowledge of incident, but no media attention •Client/Customer concerns •TMX is linked to negative news coverage, but is not the catalyst	•Verbal warnings from Regulators •Potential Litigation $10 to $50 Million	•Some staff morale problems •Significant impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $50K to $100K
5	Very Low	•Direct loss or cost of up to 1-5% of annual earnings	•Reputation intact, internal knowledge only •Minimal or no impact on customers •Letters containing negative sentiments sent to senior management and the Board	•Regulatory requirements not met •No reprimand or special undertaking •Potential Litigation between $1 and $10 Million	•Operating loss including damage to third party property <$50K •Some impact on the provision of critical services

Security Incident Condition (SICON)

SICON Title	Security Incident Conditions (SICON)
Very High	• Confirmed Security Breach, or • Confirmed Deliberate or Non-Deliberate Attacks with imminent Security Breach if action is not taken
High	• Confirmed Deliberate Attacks but Security Breach is not imminent, or • Security Incidents reported by a Trusted Source, or expected
Medium	• Suspected Deliberate Attacks,or reported by a Non-Trusted Source • Widespread known malware infestation, or • Confirmed Non-Deliberate Attacks
Low	• Localized known malware infection, or • Significant Vulnerability or Threat Agent identified
Very Low	• After analysis, conclusion that no Deliberate or Non-Deliberate Attacks have occurred or will occur. **Used as a "downgrade" mechanism for previously suspected Security Incident

Validate Phase



Security Incident Severity Level Matrix

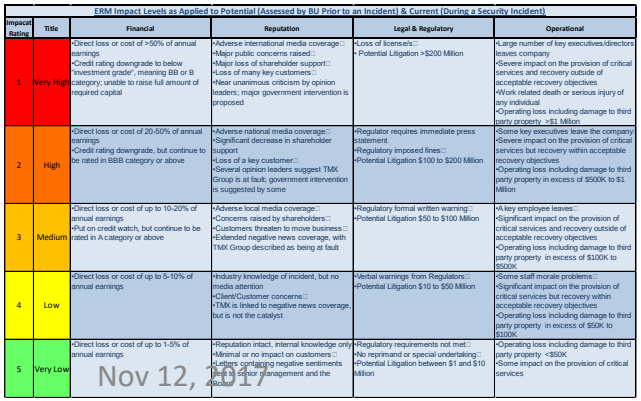
Assessed Combined "Potential Impact"	Assessed Combined "Current Impact"	Security Incident Condition (SICON)					Minimum Security Level Incident
		Very High	High	Medium	Low	Very Low	
Very High	Very High	1	2	3	4	Close Ticket	
Very High	High	1	2	3	4	Close Ticket	
Very High	Medium	2	3	4	4	Close Ticket	
Very High	Low	3	4	4	4	Close Ticket	
Very High	Very Low	4	4	4	4	Close Ticket	
High	Very High	1	2	3	4	Close Ticket	
High	High	2	2	3	4	Close Ticket	
High	Medium	3	3	4	4	Close Ticket	
High	Low	4	4	4	4	Close Ticket	
High	Very Low	4	4	4	4	Close Ticket	
Medium	Very High	n/a	n/a	n/a	n/a	Close Ticket	
Medium	High	2	3	4	4	Close Ticket	
Medium	Medium	3	3	4	4	Close Ticket	
Medium	Low	4	4	4	4	Close Ticket	
Medium	Very Low	4	4	4	4	Close Ticket	
Low	Very High	n/a	n/a	n/a	n/a	Close Ticket	
Low	High	n/a	n/a	n/a	n/a	Close Ticket	
Low	Medium	3	4	4	4	Close Ticket	
Low	Low	4	4	4	4	Close Ticket	
Low	Very Low	4	4	4	4	Close Ticket	
Very Low	Very High	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	High	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	Medium	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	Low	4	4	4	4	Close Ticket	
Very Low	Very Low	4	4	4	4	Close Ticket	

BU Potential Impact for Assets

Determine SI Severity Level

SICON

Current Impact

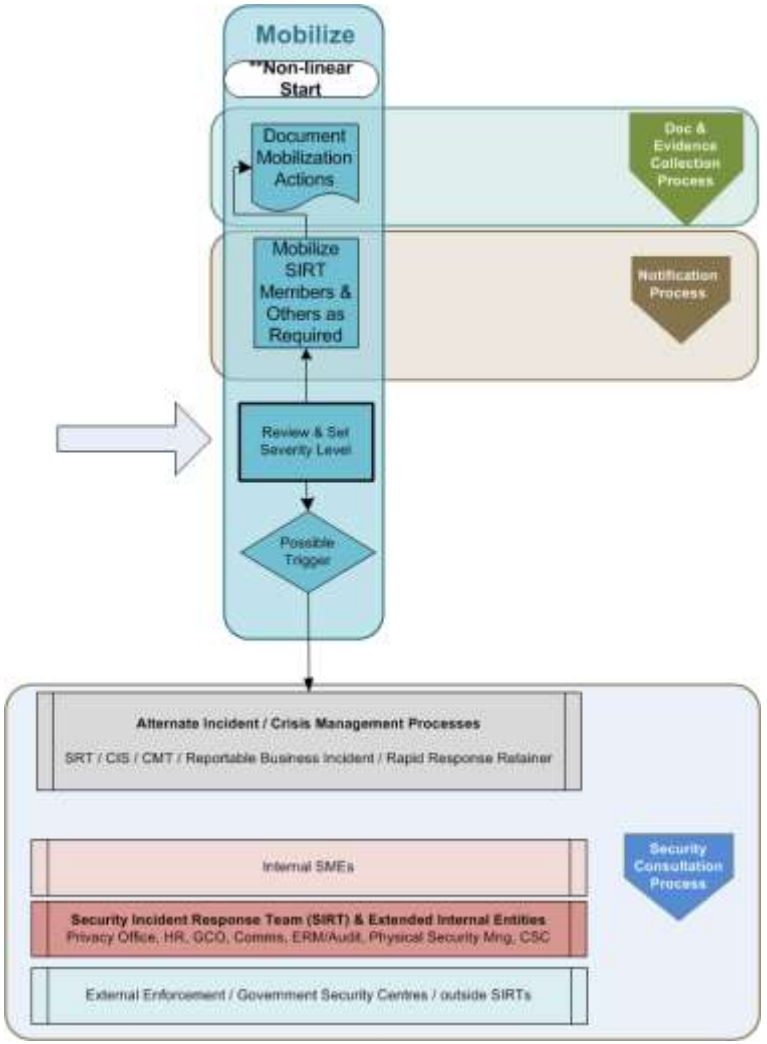


Assessed Combined "Potential Impact"	Assessed Combined "Current Impact"	Security Incident Condition (SICON)					SI Severity Rating
		Very High	High	Medium	Low	Very Low	
Very High	Very High	1	2	3	4	Close Ticket	1
Very High	High	1	2	3	4	Close Ticket	
Very High	Medium	2	3	4	4	Close Ticket	
Very High	Low	3	4	4	4	Close Ticket	
Very High	Very Low	4	4	4	4	Close Ticket	
High	Very High	1	2	3	4	Close Ticket	2
High	High	2	2	3	4	Close Ticket	
High	Medium	3	3	4	4	Close Ticket	
High	Low	4	4	4	4	Close Ticket	
High	Very Low	4	4	4	4	Close Ticket	
Medium	Very High	n/a	n/a	n/a	n/a	Close Ticket	
Medium	High	2	3	4	4	Close Ticket	
Medium	Medium	3	3	4	4	Close Ticket	
Medium	Low	4	4	4	4	Close Ticket	
Medium	Very Low	4	4	4	4	Close Ticket	
Low	Very High	n/a	n/a	n/a	n/a	Close Ticket	3
Low	High	n/a	n/a	n/a	n/a	Close Ticket	
Low	Medium	3	4	4	4	Close Ticket	
Low	Low	4	4	4	4	Close Ticket	
Low	Very Low	4	4	4	4	Close Ticket	
Very Low	Very High	n/a	n/a	n/a	n/a	Close Ticket	4
Very Low	High	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	Medium	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	Low	4	4	4	4	Close Ticket	5
Very Low	Very Low	4	4	4	4	Close Ticket	

ERM Impact Levels as Applied to Potential (Assessed by BU Prior to an Incident) & Current (During a Security Incident)

Impact Rating	Title	Financial	Reputation	Legal & Regulatory	Operational
1	Very High	•Direct loss or cost of >50% of annual earnings •Credit rating downgrade to below "investment grade", meaning BB or B category; unable to raise full amount of required capital	•Adverse international media coverage:: •Major public concerns raised:: •Major loss of shareholder support:: •Loss of many key customers:: •Near unanimous criticism by opinion leaders; major government intervention is proposed	•Loss of license/s:: • Potential Litigation >$200 Million	•Large number of key executives/directors leaves company •Severe impact on the provision of critical services and recovery outside of acceptable recovery objectives •Work related death or serious injury of any individual •Operating loss including damage to third party property >$1 Million
2	High	•Direct loss or cost of 20-50% of annual earnings •Credit rating downgrade, but continue to be rated in BBB category or above	•Adverse national media coverage:: •Significant decrease in shareholder support •Loss of a key customer:: •Several opinion leaders suggest TMX Group is at fault; government intervention is suggested by some	•Regulator requires immediate press statement •Regulatory imposed fines:: •Potential Litigation $100 to $200 Million	•Some key executives leave the company •Severe impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $500K to $1 Million
3	Medium	•Direct loss or cost of up to 10-20% of annual earnings •Put on credit watch, but continue to be rated in A category or above	•Adverse local media coverage:: •Concerns raised by shareholders:: •Customers threaten to move business:: •Extended negative news coverage, with TMX Group described as being at fault	•Regulatory formal written warning:: •Potential Litigation $50 to $100 Million	•A key employee leaves:: •Significant impact on the provision of critical services and recovery outside of acceptable recovery objectives •Operating loss including damage to third party property in excess of $100K to $500K
4	Low	•Direct loss or cost of up to 5-10% of annual earnings	•Industry knowledge of incident, but no media attention •Client/Customer concerns:: •TMX is linked to negative news coverage, but is not the catalyst	•Verbal warnings from Regulators:: •Potential Litigation $10 to $50 Million	•Some staff morale problems:: •Significant impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $50K to $100K
5	Very Low	•Direct loss or cost of up to 1-5% of annual earnings	•Reputation intact, internal knowledge only •Minimal or no impact on customers:: •Letters containing negative sentiments sent to senior management and the Board	•Regulatory requirements not met:: •No reprimand or special undertaking:: •Potential Litigation between $1 and $10 Million	•Operating loss including damage to third party property <$50K •Some impact on the provision of critical services

Mobilize Phase



Security Incident Response Levels

SI Severity Rating	SI Response Title	Security Incident Response
1	Immediate/ Continuous Response	• Justifies immediate management attention and dedicated resources applying continuous efforts to resolve as soon as possible • Full SIRT deployed including liason with CISO, IT Manager and ERM • CISO may execute Rapid Response Retainer • CISO invokes Emergency Management Team (EMT)
2	Priority Response	• Justifies priority attention and application of resources to resolve in a timely manner • Full SIRT deployed including liason with CISO and IT Incident Manager • Other liasons established as required
3	Timely Response	• Requires timely resolution to minimize future impacts • SIRT Manager and Security Operations Manager deployed
4	BAU Response	• BAU resolution through IT Incident Management • SIRT Manager deployed • Liasons as required
5	Downgraded	• Downgrade from previously suspected Security Incident to Adverse Event. • SIRT Manager already deployed • Security Ticket closed as False Positive

Security Incident Notification Timings

SI Severity Rating	Initial Notification to Distribution Lists	Update Notifications to Distribution Lists
1	• 15 minutes after Security Incident declared, or change to Severity Level 1 • Formal email and either phone call or pager notification from SIRT	• Every 30 minutes until Security Ticket is closed or until Severity Level is reduced • Formal email notification from SIRT
2	• 30 minutes after Security Incident declared, or change to Severity Level 2 • Formal email and either phone call or pager notification from SIRT	• Every 60 minutes until Security Ticket is closed or until Severity Level is reduced • Formal email notification from SIRT
3	• 60 minutes after Security Incident declared, or change to Severity Level 3 • Formal email notification from SIRT	• Every 24 hours until Security Ticket is closed or until Severity Level is reduced • Formal email notification from SIRT
4	• 24 hours after Security Incident declared, or change to Severity Level 4 • Email notification from SIRT	• Upon resolution or until Severity Level is reduced • Email notification from SIRT
5	N/A	N/A

Seniority of SIRT Members

SIM Actors, Roles, Teams, Entities	Validate					Mobilize					Respond					Eradicate & Recover					Close					Post Mortem					Cross-Phase Processes		
	Sev 5	Sev 4	Sev 3	Sev 2	Sev 1	Sev 5	Sev 4	Sev 3	Sev 2	Sev 1	Sev 5	Sev 4	Sev 3	Sev 2	Sev 1	Sev 5	Sev 4	Sev 3	Sev 2	Sev 1	Sev 5	Sev 4	Sev 3	Sev 2	Sev 1	Sev 5	Sev 4	Sev 3	Sev 2	Sev 1	Documentation	Notification	Evidence Collection
SIRT Roles																																
Security Ticket Owner	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R						AR		R
SIRT Manager		AR	AR	AR	AR		AR	AR	AR	AR		AR	AR	AR	AR		AR	AR	AR	AR		AR	AR	AR	AR						C	AR	AR
BU SIRT (BSIRT) Manager								C	R	R			C	R	R			C	R	R			C	R	R							C	R	R
SOM (Security Operations Manager)								R	R	R			R	R	R			R	R	R			R	R	R							C	R	R
External Rapid Response Retainer (EXTVENDOR1) if Severity 1 or as needed										AR					AR					AR					AR					AR	AR	AR	AR
Exernal Forensics Vendor (EXTVENDOR2) if Severity 1 or as needed										R					R					R					R					R			AR
SIRT Shared Services																																	
ABC CISO (to EMT, External Rapid Response)				O	M				O	M				O	M				O	M				O	M				O	M			O
IT Incident Manager(to SRT/IRT, CIS, EMT)			O	O	M			O	O	M			O	O	M			O	O	M			O	O	M			O	O	M			O
Affected BU Security Council Member(s)			O	M	M			O	M	M			O	M	M			O	M	M			O	M	M			O	O	M			O
ERM (to Risk Case Management, EMT)					M					M					M					M					M				O	M			O
Privacy Manager			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O
HR			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O
GCO (also to liase with External Enforcement, Regulators, any other outside entity)			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O
Comms			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O
Physical Security Mng			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O	O	O			O

Process Accountabilities — Accountable, Responsible, Consulted, Informed

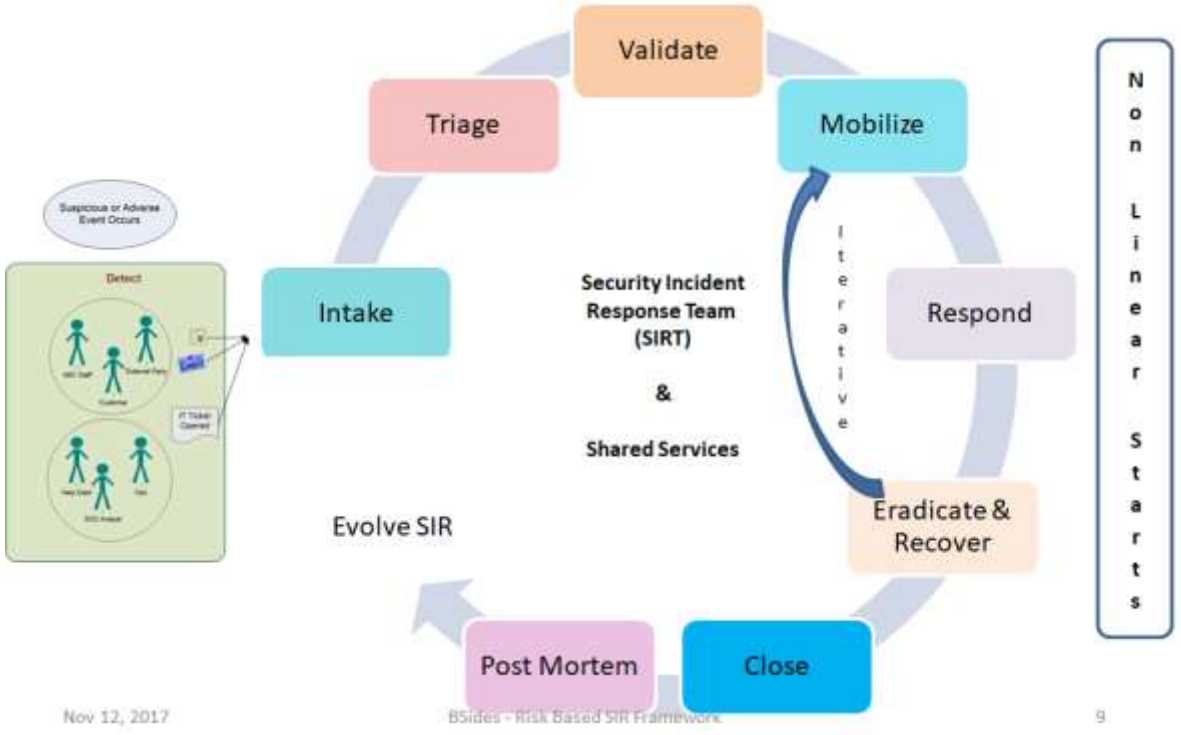
Shared Services Involvement — + Only as Required, Mandatory

SI Notification Distribution Lists

Security Incident Severity	Operations - Production Support	SOC Level 1	SOC Level 2	SOC Level 3	SIRT & BSIRT Manager	Security Operations Manager	Full SIRT	CISO	IT Incident Manager	Affected BU Security Council Member(s)	IT Service Response Team	Shared Services & Risk Mgmt	Emerg Mgmt Team	External Rapid Response	3rd Parties
1	O	M	M	M	M	M	M	M	M	M	M	M	M	M	O
2	O	O	M	M	M	M	M	O	O	M	O	O	O	O	O
3	O	O	M	O	O	O	O	O	O	O	O				
4	O	O	O	O											
*5	O	O	O	O											

"O" Only as required "M" Mandatory *Very Low is used only when downgrading an existing Security Ticket

The SIRT continues to next phases



But to recap….

BU Potential Impact for Assets

Set Required Seniority of SIRT Members

Determine SI Severity Level

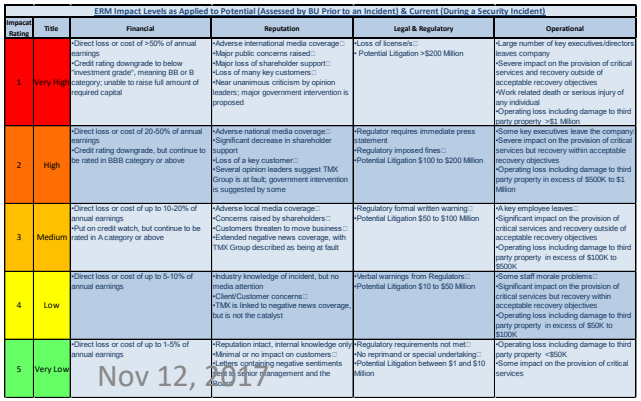
Assessed Combined "Potential Impact"	Assessed Combined "Current Impact"	Security Incident Condition (SICON)					SI Severity Rating
		Very High	High	Medium	Low	Very Low	
Very High	Very High	1	2	3	4	Close Ticket	1
Very High	High	1	2	3	4	Close Ticket	
Very High	Medium	2	3	4	4	Close Ticket	
Very High	Low	3	4	4	4	Close Ticket	
Very High	Very Low	4	4	4	4	Close Ticket	
High	Very High	1	2	3	4	Close Ticket	
High	High	2	2	3	4	Close Ticket	
High	Medium	3	3	4	4	Close Ticket	
High	Low	4	4	4	4	Close Ticket	
High	Very Low	4	4	4	4	Close Ticket	
Medium	Very High	n/a	n/a	n/a	n/a	Close Ticket	2
Medium	High	2	3	4	4	Close Ticket	
Medium	Medium	3	3	4	4	Close Ticket	
Medium	Low	4	4	4	4	Close Ticket	
Medium	Very Low	4	4	4	4	Close Ticket	
Low	Very High	n/a	n/a	n/a	n/a	Close Ticket	3
Low	High	n/a	n/a	n/a	n/a	Close Ticket	
Low	Medium	3	4	4	4	Close Ticket	
Low	Low	4	4	4	4	Close Ticket	
Low	Very Low	4	4	4	4	Close Ticket	
Very Low	Very High	n/a	n/a	n/a	n/a	Close Ticket	4
Very Low	High	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	Medium	n/a	n/a	n/a	n/a	Close Ticket	
Very Low	Low	4	4	4	4	Close Ticket	5
Very Low	Very Low	4	4	4	4	Close Ticket	

SICON

Select Level of Response

SI Response Title	Security Incident Response
Immediate/ Continuous Response	• Justifies immediate management attention and dedicated resources applying continuous efforts to resolve as soon as possible • Full SIRT deployed including liason with CISO, IT Manager and ERM • CISO may execute Rapid Response Retainer • CISO invokes Emergency Management Team (EMT)
Priority Response	• Justifies priority attention and application of resources to resolve in a timely manner • Full SIRT deployed including liason with CISO and IT Incident Manager • Other liasons established as required
Timely Response	• Requires timely resolution to minimize future impacts • SIRT Manager and Security Operations Manager deployed
BAU Response	• BAU resolution through IT Incident Management • SIRT Manager deployed • Liasons as required
Downgraded	• Downgrade from previously suspected Security Incident to Adverse Event • SIRT Manager already deployed • Security Ticket closed as False Positive

Current Impact

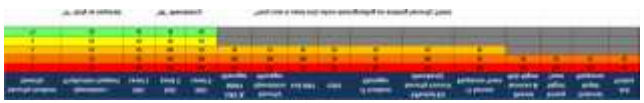


Impact Rating	Title	Financial	Reputation	Legal & Regulatory	Operational
1	Very High	•Direct loss or cost of >50% of annual earnings •Credit rating downgrade to below "investment grade", meaning BB or B category; unable to raise full amount of required capital	•Adverse international media coverage:: •Major public concerns raised:: •Major loss of shareholder support:: •Loss of many key customers:: •Near unanimous criticism by opinion leaders; major government intervention is proposed	•Loss of licenses\:\: • Potential Litigation >$200 Million	•Large number of key executives/directors leaves company •Severe impact on the provision of critical services and recovery outside of acceptable recovery objectives •Work related death or serious injury of any individual •Operating loss including damage to third party property >$1 Million
2	High	•Direct loss or cost of 20-50% of annual earnings •Credit rating downgrade, but continue to be rated in BBB category or above	•Adverse national media coverage:: •Significant decrease in shareholder support •Loss of a key customer:: •Several opinion leaders suggest TMX Group is at fault; government intervention is suggested by some	•Regulator requires immediate press statement •Regulatory imposed fines:: •Potential Litigation $100 to $200 Million	•Some key executives leave the company •Severe impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $500K to $1 Million
3	Medium	•Direct loss or cost of up to 10-20% of annual earnings •Put on credit watch, but continue to be rated in A Category or above	•Adverse local media coverage:: •Concerns raised by shareholders:: •Customers threaten to move business:: •Extended negative news coverage, with TMX Group described as being at fault	•Regulatory formal written warning:: •Potential Litigation $50 to $100 Million	•A key employee leaves:: •Significant impact on the provision of critical services and recovery outside of acceptable recovery objectives •Operating loss including damage to third party property in excess of $100K to $500K
4	Low	•Direct loss or cost of up to 5-10% of annual earnings	•Industry knowledge of incident, but no media attention •Client/Customer concerns:: •TMX is linked to negative news coverage, but is not the catalyst	•Verbal warnings from Regulators:: •Potential Litigation $10 to $50 Million	•Some staff morale problems:: •Significant impact on the provision of critical services but recovery within acceptable recovery objectives •Operating loss including damage to third party property in excess of $50K to $100K
5	Very Low	•Direct loss or cost of up to 1-5% of annual earnings	•Reputation intact, internal knowledge only •Minimal or no impact on customers:: •Letters containing negative sentiments sent to senior management and the Board	•Regulatory requirements not met:: •No reprimand or special undertaking:: •Potential Litigation between $1 and $10 Million	•Operating loss including damage to third party property <$50K •Some impact on the provision of critical services

Determine Notification Schedule

Initial Notification to Distribution Lists	Update Notifications to Distribution Lists
• 15 minutes after Security Incident declared, or change to Severity Level 1 • Formal email and either phone call or pager notification from SIRT	• Every 30 minutes until Security Ticket is closed or until Severity Level is reduced • Formal email notification from SIRT
• 30 minutes after Security Incident declared, or change to Severity Level 2 • Formal email and either phone call or pager notification from SIRT	• Every 60 minutes until Security Ticket is closed or until Severity Level is reduced • Formal email notification from SIRT
• 60 minutes after Security Incident declared, or change to Severity Level 3 • Formal email notification from SIRT	• Every 24 hours until Security Ticket is closed or until Severity Level is reduced • Formal email notification from SIRT
• 24 hours after Security Incident declared, or change to Severity Level 4 • Email notification from SIRT	• Upon resolution or until Severity Level is reduced • Email notification from SIRT
N/A	N/A

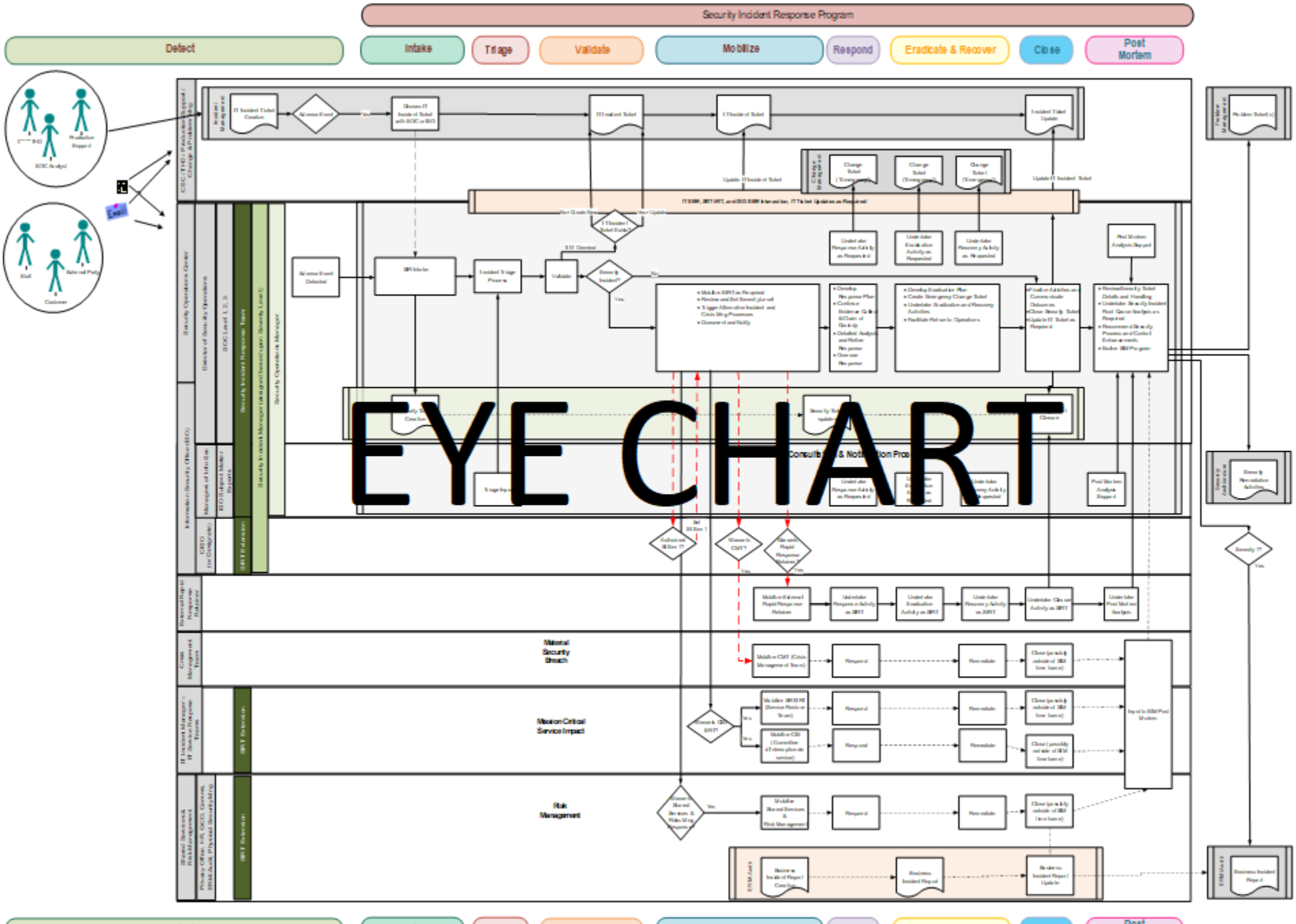
Determine Notification Addresses



Questions?

Keith Jonah
CISSP, CISM, CRISC
kjonah@trustedbydesign.ca
416.727.3809

Kevin Pietersma
CISSP, SANS GCIA Gold
@bydasein
647.284.5387


Security Incident Response Program
Detect
Intake
Triage
Validate
Mobilize
Respond
Eradicate & Recover
Close
Post Mortem
EYE CHART
Email
Internal Security Breach
Mission Critical Service Impact
Risk Management
Detect
Intake
Triage
Validate
Mobilize
Respond
Eradicate & Recover
Close
Post Mortem