PI and Databases:
An opportunity for Discussion

Gila Pyke

Smart Systems for Health Agency
September, 2006

Ontario
Smart Systems
for Health Agency

Personal Information (PI) is *complicated*.

Databases (DB) are *complicated*.

Ergo: PI + DB = *Complicated*^{2}

PI + DB Risks, Issues, Root Causes, etc.

Identity Theft

Identity *Loss*

Fear

Service disruption

Privacy Breach

Data conflicts

Complexity

Anything else?

PI + DB Opportunities: A mixed bag

Reduce costs and response times
(Faster FOI response times)

Inherent audit trail = accountability

Automating incident response

Reduction in impact on the individual

Reduction in breaches

Accuracy and efficiency, reduction in duplicate records, conflicting records (the no-fly list!)

So why do we do it? Inertia? Idealism? Improving service delivery?

Why do *you* do it?

Success Stories

Changing culture: From auditors to facilitators

Engagement

Awareness ("Data flow" is part of common vocabulary)

Incident response (Beyond recovery, a motivator for change)

What are *your* success stories?

So what should I do?

Know your Information Inventory + Data flow

What are my impacts?

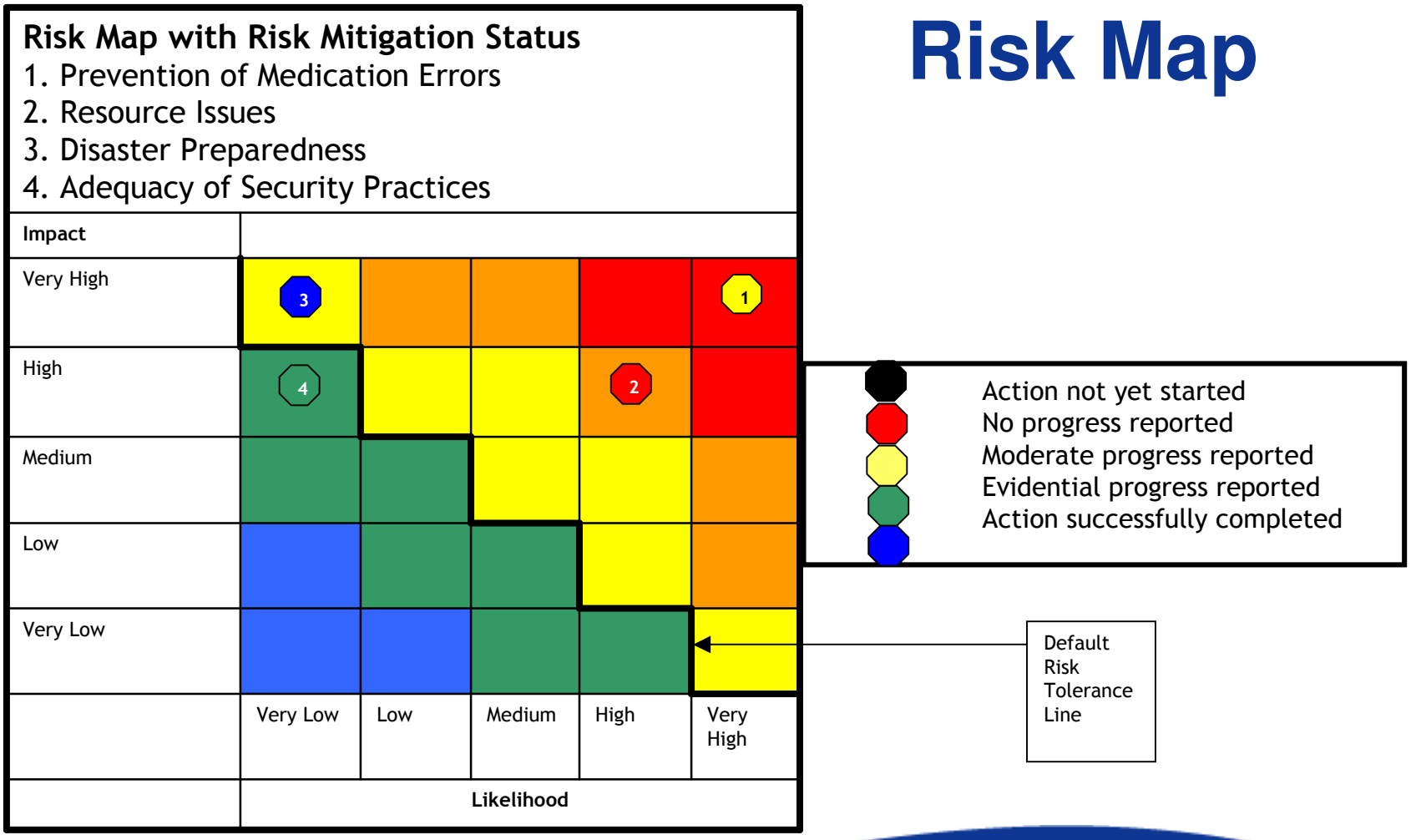
	Cost	Reputation	Safety	Delivery	
Very High	Capital Cost of > $100 M	Potential for reduction in SSHA mandate	Potential for multiple fatalities / serious injuries	Six months or more	May not be able to deliver on most critical requirements
High	Capital Cost of $10M to $100 M	Serious adverse attention from media, medical establishment and / or public	Potential for single fatality / serious injury	Between two and six months	Major shortfalls in one or more critical requirements
Medium	Capital Cost of $1M to $10 M	Minor adverse attention from media, medical establishment and / or public	Potential for minor injury	Between two weeks and two months	Minor shortfalls in one or more key requirements
Low	Capital Cost of $100,000 to $1M	Loss of reputation among clients / partners	Potential to reduce quality of health care	Less than two weeks	A few shortfalls in desired functionality
Very Low	Capital Cost of < $100,000	Internal loss of reputation	Impact does not affect delivery of health care	Less than two days	System should still fully meet mandatory requirements

Let's be honest about probability

Very High	>80%
High	More likely than not: 51-79%
Medium	Fairly Likely: 21-50%
Low	Unlikely: 6-20%
Very Low	Virtually Impossible <5%

Be clear, even *visual* about priorities

Risk Map



Information Design Concepts

- Collect only what I need (Data minimization)
- Encryption
- Personal identifiers
  - Segregate them
  - *Pseudo*nimize them
- Data aggregation and *anon*ymization

Consider Collection

What are your use cases?

- Expected types of information
- Expected disclosures
- Expected uses for information
  - Will we do *data matching*?
  - Data *sharing*?
  - Do I need consent ? Notification?
  - What are my retention schedules?

Do I expect my use cases to change? When?

Who are the owners? Custodians?

Consider Control

- Access Control
  - Role based
  - Authentication (2 factor, 3 factor)
  - Authorization
- Auditability
- FOI usability
- Accuracy
- Incident areas
  - What are your breach and investigation scenarios?

Don’t forget:

- Make time to consult all your stakeholders, *(including lawyers)*
- Information Classification (Sensitivity)
- Metrics: Is it doing what we designed it to do?
- Usability (Font Size!)
- Dates – Status – Optimized Queries – Administrative Data

Anything else?

Sign up for our e-newsletter at www.ssha.on.ca