Visibility Analysis and Management

Jack Jones, CISM, CISSP, CISA
RMI Founder
Ignorance is not bliss
What we’ll cover...

- What do we mean by “visibility”?
- Whose visibility are we concerned with?
- Evaluating visibility
- Gaining visibility
- Maintaining visibility
- Q&A
What do we mean by “visibility”?
When is something “visible”?
When is something “visible”?

If you have and can maintain enough information about a component of your environment that you accurately understand its risk significance, then it is “visible” to you.
Visibility criteria
Visibility criteria

• For an asset to be visible, you have to know:
  ‣ That it exists
Visibility criteria

- For an asset to be visible, you have to know:
  - That it exists
  - Its value/liability characteristics
Visibility criteria

• For an asset to be visible, you have to know:
  ‣ That it exists
  ‣ Its value/liability characteristics
  ‣ The threat landscape it faces
Visibility criteria

• For an asset to be visible, you have to know:
  ‣ That it exists
  ‣ Its value/liability characteristics
  ‣ The threat landscape it faces
  ‣ Its control condition
Whose visibility matters?
Whose visibility matters?
Whose visibility matters?

It’s all about decision-making.
Whose visibility matters?

It’s all about decision-making.

The decision-maker either has to have visibility, or the person providing them the information they base their decision on has to have visibility.
Key decisions
Key decisions

• Prioritization
Key decisions

• Prioritization

• Solution comparison and selection
Key decisions

- Prioritization
- Solution comparison and selection
- Strategy development
Evaluating visibility
Evaluating visibility
Evaluating visibility

- Two components:
  - Carving up the landscape into “asset groups”
  - Evaluating the asset groups
Carving up the landscape
Carving up the landscape

- Identify the asset components that make up your landscape, for example:
  - Internet PoP’s
  - 3rd party connections
  - Internet applications
  - Windows servers
  - Development and test environments
  - Legacy applications
  - Managed databases
  - Unmanaged databases
  - Etc…
Carving up the landscape
Carving up the landscape

• **NOTE**: You may need to start by gaining visibility into the business itself
  - Lines of business
  - Business processes
  - Departments
  - Locations
  - Business relationships
  - Personnel
Prioritizing visibility
Prioritizing visibility

• Don’t eat the elephant all at once. Prioritize, based on perceived:
  ‣ Value/liability
  ‣ Threat levels
  ‣ Control conditions
  ‣ Frequency of change
Evaluating visibility
Evaluating visibility

• For each asset group, ask the question:
  ‣ “What percentage of [asset group] do you have visibility into?”
Evaluating visibility

• For each asset group, ask the question:
  ‣ “What percentage of [asset group] do you have visibility into?”

• Make certain all aspects of visibility are considered
Evaluating visibility

• For each asset group, ask the question:
  ‣ “What percentage of [asset group] do you have visibility into?”

• Make certain all aspects of visibility are considered

• Estimate minimum, maximum, and most likely visibility
  ‣ Preferably get calibrated estimates
Evaluating visibility
Evaluating visibility

• For example:
  ▶ “What percentage of unmanaged databases do we have visibility into?”
    - Minimum: 10% (one out of ten)
    - Maximum: 25% (one out of four)
    - Most likely: 20% (one out of five)
Evaluating visibility

• For example:
  ‣ “What percentage of unmanaged databases do we have visibility into?”
    - Minimum: 10% (one out of ten)
    - Maximum: 25% (one out of four)
    - Most likely: 20% (one out of five)

• Why bother with a range?
Visibility

Certainty

Two Dimensions
How do we gain visibility?
Gaining visibility
Gaining visibility

• Example - Unmanaged Databases:
  ▸ Starting visibility: 10% to 25%
Example - Unmanaged Databases:

- Starting visibility: 10% to 25%
- What are the options for improving visibility?
Gaining visibility

• Example - Unmanaged Databases:
  ‣ Starting visibility: 10% to 25%
  ‣ What are the options for improving visibility?
  ‣ Are there current tools/processes/people in the organization that we can leverage?
Gaining visibility

- Example - Unmanaged Databases:
  - Starting visibility: 10% to 25%
  - What are the options for improving visibility?
  - Are there current tools/processes/people in the organization that we can leverage?
  - Set specific objectives
Gaining visibility

• Example - Unmanaged Databases:
  ‣ Starting visibility: 10% to 25%
  ‣ What are the options for improving visibility?
  ‣ Are there current tools/processes/people in the organization that we can leverage?
  ‣ Set specific objectives
    - e.g. 90% minimum by March 1, 2011
Gaining visibility
Gaining visibility

• The good news...
  ‣ Simply asking the questions about visibility often highlights which data you need, and from where, in order to improve visibility
Gaining visibility

• The good news...
  ‣ Simply asking the questions about visibility often highlights which data you need, and from where, in order to improve visibility
  ‣ You can start simple and make significant gains without a lot of cost/effort.
Gaining visibility

• The good news...
  ‣ Simply asking the questions about visibility often highlights which data you need, and from where, in order to improve visibility
  ‣ You can start simple and make significant gains without a lot of cost/effort.
  ‣ These are actually useful metrics
Gaining visibility
Gaining visibility

• The “bad” news...
  ‣ Some data are harder to come by than others
Risk Landscape Visibility
How do we maintain visibility?
Maintaining visibility
Maintaining visibility

• Can be a very different problem than gaining initial visibility
Maintaining visibility

• Can be a very different problem than gaining initial visibility

• Two approaches:
  ‣ Active maintenance
  ‣ Periodic updates
Maintaining visibility

• Can be a very different problem than gaining initial visibility

• Two approaches:
  ‣ Active maintenance
  ‣ Periodic updates

• How often do you need to update our visibility?
  ‣ Realtime?
  ‣ Quarterly?
  ‣ Annually?
Timeliness consideration
Timeliness consideration

- Timeliness is mostly about frequency...
  - of change, and
  - of threat events
Control effectiveness vs Time
Time

Control effectiveness

Implementation
Control effectiveness

Implementation

Change occurs

Time
Control effectiveness

Implementation

Change occurs

Remediation

Threat event

Time

Threat event
Control effectiveness

Implementation

Change occurs

Remediation

Threat event

Time

Threat event
Maintaining visibility
Maintaining visibility

• Leverage existing technologies & processes
Maintaining visibility

• Leverage existing technologies & processes
• Establish policies regarding asset registration
Maintaining visibility

• Leverage existing technologies & processes
• Establish policies regarding asset registration
• Integrate with:
  ‣ Project management
  ‣ Change management
  ‣ BCP/DR
Maintaining visibility

• Leverage existing technologies & processes
• Establish policies regarding asset registration
• Integrate with:
  ‣ Project management
  ‣ Change management
  ‣ BCP/DR
• Establish policies regarding asset registration
Summary
Summary

• Visibility is required in order to:
  ‣ Make well-informed risk decisions
  ‣ Rationally claim that you are actually managing risk
Summary

• Visibility is required in order to:
  ‣ Make well-informed risk decisions
  ‣ Rationally claim that you are actually managing risk

• You have to carve up the landscape into asset groups in order to make your estimates.
Summary

• Visibility is required in order to:
  ‣ Make well-informed risk decisions
  ‣ Rationally claim that you are actually managing risk

• You have to carve up the landscape into asset groups in order to make your estimates.

• In order for an asset group to be “visible” you have to know its risk significance
Summary

• Visibility is required in order to:
  ‣ Make well-informed risk decisions
  ‣ Rationally claim that you are actually managing risk

• You have to carve up the landscape into asset groups in order to make your estimates.

• In order for an asset group to be “visible” you have to know its risk significance

• Don’t try to eat the entire elephant at once. Prioritize your visibility efforts based on “risk potential”
Summary
Summary

• Leverage existing technology/processes/people as much as possible
Summary

• Leverage existing technology/processes/people as much as possible

• Once you’ve established decent visibility, establish a strategy for maintaining it
Summary

- Leverage existing technology/processes/people as much as possible
- Once you’ve established decent visibility, establish a strategy for maintaining it
- “Visibility” is just another way of thinking about, evaluating, and managing our problem space
Questions?

If you’d like help establishing visibility within your organization, or for more information about RMI’s services:

www.riskmanagementinsight.com
info@riskmanagementinsight.com
888-416-5722