RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-W04

How Infosec Maturity Models are Missing the Point

Jack Jones

EVP R&D
RiskLens, Inc.
@jonesFAIRiq

What makes infosec so challenging?

Complex landscape

Dynamic landscape

Inherent conflict with an organization's need/desire to limit costs

What we'll cover…

- What does maturity look like?
- What's missing in common maturity models
- The cost of immaturity
- Maturity measurement
- Recommended steps

What does “maturity” look like?

What are some common “maturity” indicators?

Common example characteristics…

- Policies based on “best practices”
- Regular reporting to the board of directors (executive management)
- Has a metrics program
- Uses threat intelligence
- Regular awareness training
- etc…

Can an organization have these characteristics and still be ineffective?

What's missing in common maturity models?

What are we really trying to measure?

The ability of an organization to cost-effectively manage information security risk over time.

“Cost-Effectively”

- Implies…
  - Prioritizing effectively
  - Choosing the most cost-effective solutions
  - Prevention/correction of systemic problems
- Depends upon…
  - Effective risk measurement
  - Effective root cause analysis

“Over time”

- Implies…
  - Repeatable
  - Managing change in the risk landscape (where/when possible)
  - Adjusting to changes in the risk landscape (when outside of its control)
- Depends upon…
  - Reliable execution
  - Well informed decisions

Which of the following are risks?

- Disgruntled insiders
- Internet-facing web servers
- Untested recovery processes
- Network shares containing sensitive consumer information
- Weak passwords
- Hurricane force winds

Which of the following are risks?

None of them are!

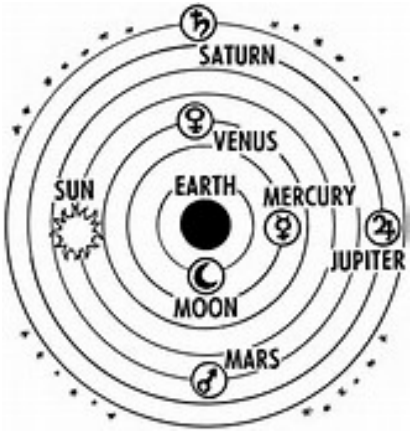
- Disgruntled insiders — Threats
- Internet-facing web servers — Assets
- Untested recovery processes — Control deficiency
- Network shares containing sensitive consumer information — Assets
- Weak passwords — Control deficiency
- Hurricane force winds — Threats

First missing element…

You can't measure or manage what you haven't clearly defined.

When was the last time a maturity model included anything related to whether an organization had standardized on a logically consistent set of risk-related terms?

Second missing element…



There are “models” and then there are models.

When was the last time a maturity model included anything related to the quality of models being used to perform risk analysis?

Third missing element…

Critical thinking
Estimation skills
Analysis scoping

Analytic capabilities.

When was the last time a maturity model included anything related to personnel being trained in analysis?

Fourth missing element…

Root cause analysis

When was the last time a maturity model included anything related to the quality of root cause analysis?

The cost of immaturity

Which of the following is worst?

- Disgruntled insiders
- Internet-facing web servers
- Untested recovery processes
- Network shares containing sensitive consumer information
- Weak passwords
- Hurricane force winds

Which of the following is worst?

The question can't be answered!

- Disgruntled insiders — Threats
- Internet-facing web servers — Assets
- Untested recovery processes — Control deficiency
- Network shares containing sensitive consumer information — Assets
- Weak passwords — Control deficiency
- Hurricane force winds — Threats

Risk exists when you combine threats and assets. You can't compare these individual elements directly.

Inability to prioritize effectively

70% to 90% of the “high risk” issues I encounter within organizations turn out to NOT represent high risk.

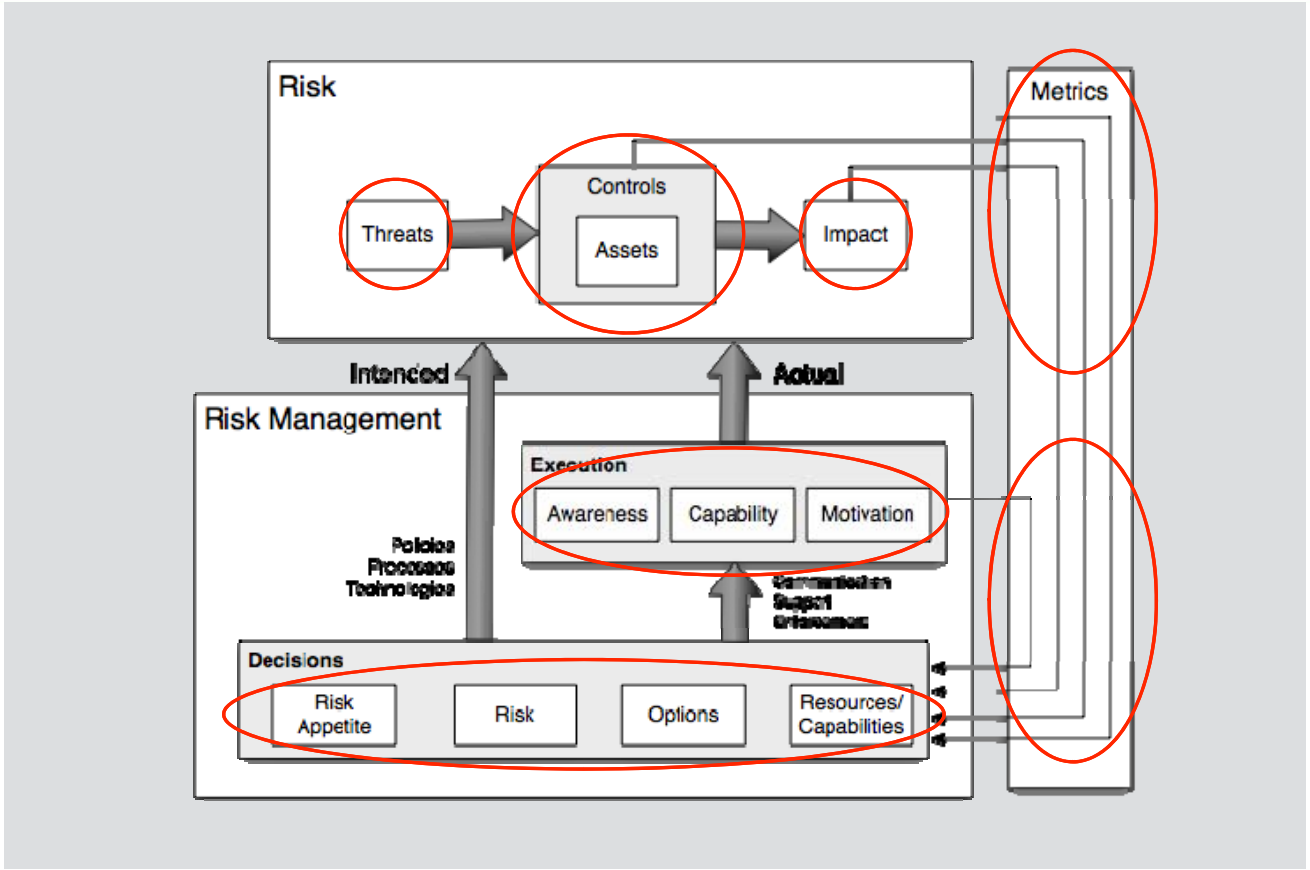
…which means they are unable to focus on the things that matter most.

Unreliable execution and wasted resources

You know you're in "risk management groundhog day" when…

You see the same problems repeatedly
…even after you've "fixed" them
…multiple times

The risk landscape as a system…



Maturity measurement

Nomenclature

- **Immature**: No standard definitions for foundational terms have been established, or the established definitions are logically inconsistent.
- **Evolving**: Logically consistent standard definitions for foundational terms have been established, however their use is inconsistent.
- **Mature**: Logically consistent standard definitions for foundational terms have been established, and their use is consistent.

Risk model

- **Immature**: Risk ratings/measurements are based on the unvetted mental models of personnel.
- **Evolving**: Risk ratings/measurements are based on an internally developed risk model that is logically consistent.
- **Mature**: Risk ratings/measurements are based on an established and publicly vetted risk model (e.g., FAIR).

Analytic skills

- **Immature**: Personnel who rate/measure risk have no specific training in risk analysis or in making calibrated estimates.
- **Evolving**: Personnel who rate/measure risk have had training in either risk analysis OR in making calibrated estimates.
- **Mature**: Personnel who rate/measure risk have had training in both risk analysis AND in making calibrated estimates.

Root cause analysis

- **Immature**: No (or superficial) root cause analysis is performed on control deficiencies.
- **Evolving**: (Deep) root cause analysis is performed on control deficiencies.
- **Mature**: Root cause analysis results are examined as a portfolio to identify systemic causes and solutions.

Recommended steps (and summary)

Applying what you have learned

- Next week you should…
  - Consider your organization's maturity using the scale presented here.
  - Document the ways immaturity negatively affects your organization.
  - Exercise your critical thinking skills.

Applying what you have learned

- In the next three months you should…
  - Add maturity measures to whatever your organization already uses to evaluate its information security program.
  - Work with stakeholders to define, socialize and implement steps to close fundamental maturity gaps in your organization.
  - Learn how to make calibrated estimates (“How to Measure Anything” by Douglas Hubbard).

Applying what you have learned

- In the next six months you should…
  - Become a change agent for our profession. Write a blog post or give a presentation to colleagues and peers that advances maturity within our profession.

Summary

- Common maturity models ignore foundational elements of maturity.
- Infosec maturity boils down to the degree to which the organization can cost-effectively manage information security risk over time.
- Nomenclature, models, analytic skills and root cause analysis are foundational elements that materially affect the maturity of an organization.
- Immaturity is a huge problem within the profession, but improving it begins with you and your organizations.

Questions?

Consider attending the Focus On session being held later!
Please fill out the session evaluation form!