RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-R02

Misinforming Management

Jack Jones

President
CXOWARE, Inc.
@JonesFAIRiq

What we'll cover…

- The single biggest risk…
- Examples of misinformation
- Common ways misinformation occurs - and how to avoid them
- The benefits of change
- Bringing it home - applying what we've covered

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Any organization's single biggest risk

#RSAC

Misinformation

- In infosec it tends to be low Signal-to-Noise ratio
  - Inability to prioritize effectively, leaving major issues unaddressed
  - Resources wasted on less important issues

Low signal-to-noise

Risk	Rating
Accidental disclosure of sensitive consumer information	High
Accidental disclosure of sensitive organization information	Medium
Malicious disclosure/breach of sensitive consumer	High
Malicious disclosure/breach of sensitive organization	Medium
Data center outage	High
Data loss/destruction	Medium
E-fraud	Low
Disclosure of personal medical information	Medium
Material financial misstatement	Low
IT project late delivery	Low
IT project quality failure	Medium
IT project budget overrun	Low
Product/service degradation	Medium
Product/service outage	High
Product/service integrity problem	Low
Regulatory audit failure	Medium
Vendor deliverable quality failure	Low
Vendor failure	Low

Examples of misinformation…

Web application scan results

"Hundreds of critical and high risk vulnerabilities"

SOX Assessment

SOX-related control deficiencies reported as material

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Common ways misinformation occurs - and how to avoid them

How many of you work in organizations that use a “risk register”?

How is it being used?

Measuring the wrong thing

- Which of the following are “risks”
  - Failure to change smoke detector batteries
  - Smoke detector fails
  - Building catches on fire

Likelihood: “Moderate”

Impact: “Severe”

Measuring the wrong thing

- Which of the following are “risks”
  - Failure to change smoke detector batteries
  - Smoke detector fails
  - Building catches on fire

Control deficiencies are not “risks”

You can’t directly assign an impact estimate to a control deficiency

Avoiding this problem

- If you're measuring things as "risk" that aren't risk, then your measurements are almost certain to be inaccurate and misleading.
- Make sure you're measuring loss events, because they're the only thing you can apply a likelihood AND impact estimate to.

Misaligned measurements

- Common mistake:
  - Estimating most common occurrence for likelihood, then worst-case for impact
    - Almost always overstates the level of risk

Avoiding this problem

- Always estimate impact first
  - Worst-case? Most common outcome?
- Rate likelihood second
- Because it forces you to clarify the event you're evaluating and helps avoid misalignment between impact and likelihood ratings

Broken measurement scales

- Three most common problems
  - Ambiguity
  - Lack of alignment with business reality
  - Compression

Which of these is worse?

- Unfavorable comments from media, minor impact to staff, no criminal implications, impact to customer service, minor legal action.
- Critical article in the media, some affect on staff, attempted (unsuccessful or minor breach) of system, significant number of customers encounter minor inconveniences, individual lawsuit expected.

Avoiding this problem

- Make certain the descriptions for each level of your scale are clearly distinguished.
- Leverage numeric values whenever possible, for example:
  - Likelihood percentages (e.g., > 50% likelihood in the next year)
  - Lost revenue, number of affected customers, duration of downtime, etc.
- Consider using fewer levels in your scale.
  - Particularly if you're using qualitative descriptions

Alignment with business reality

- Where would you draw the line for “High” financial impact (the highest level in the scale) for a “Too big to fail” financial institution?
  - $500,000
  - $2,000,000
  - $10,000,000
  - $50,000,000

Is that truly “high” impact for an organization that large?

Compression in impact ratings

- Where would you draw the line for “High” financial impact (the highest level in the scale) for a “Too big to fail” financial institution?
  - $500,000
  - $2,000,000
  - $10,000,000
  - $50,000,000

$100,000,000 impact would receive the same impact rating.

Unable to distinguish at the high end of the scale.

Likelihood compression

- Where would you draw the line for “Low” likelihood?
  - Once every two years or more
  - Once every ten years or more
  - Once every fifty years or more

A 100-year flood would receive the same likelihood rating.

Unable to distinguish at the low end of the scale.

Avoiding this problem

- Work with business stakeholders to ensure scales are aligned with the business
- Make “Compression” an explicit part of the conversation

Poor measurements/estimates

News flash!

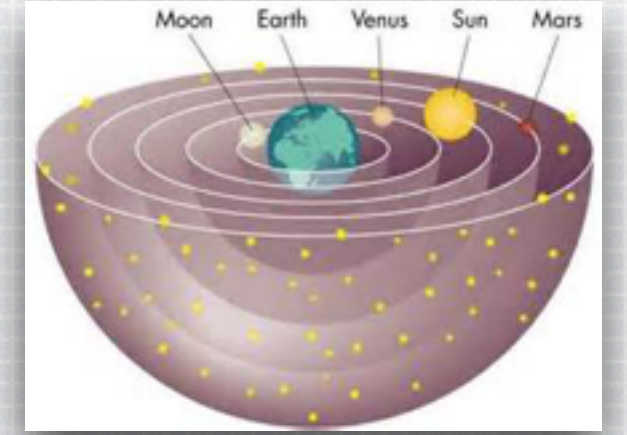
Humans stink at estimating

But they can improve dramatically with training

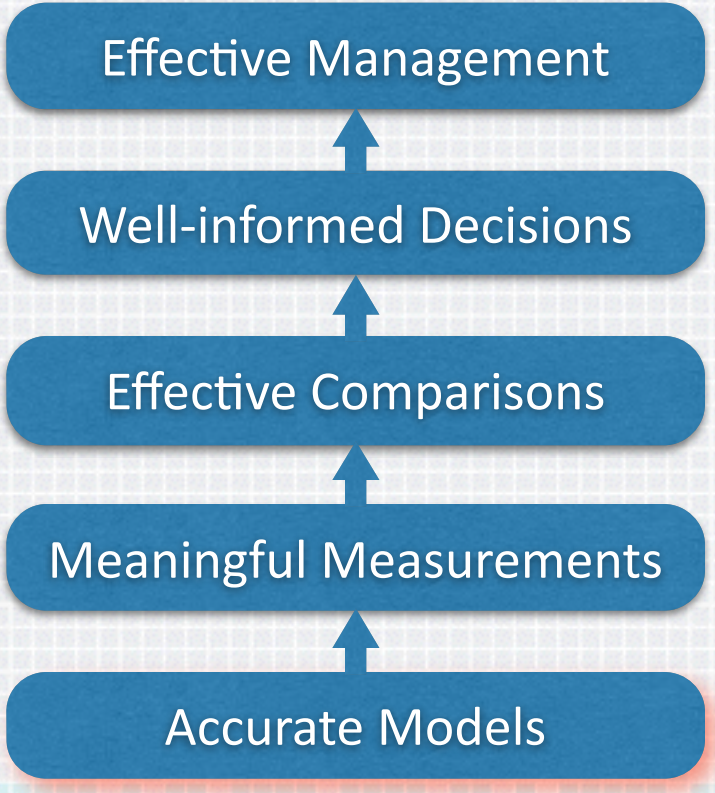
Avoiding this problem

- Get calibrated! Which is:
  - A process for gauging and improving a person's ability to make accurate estimates
  - Supports better critical thinking
- Resources
  - How to Measure Anything (by Douglas Hubbard)
  - www.lesswrong.com
  - www.predictionbook.com

Inaccurate models



Models matter



Common mistakes in infosec models

- Leaving out likelihood of an attack
- Accounting for controls in the wrong part of the equation
- Questionable math

Avoiding this problem

- Adopt an established and well-vetted public model (e.g., FAIR)

- Resources
  - The Open Group
    - http://www.opengroup.org/standards/security
    - https://www2.opengroup.org/ogsys/catalog/C13G
    - https://www2.opengroup.org/ogsys/catalog/C13K

Poor analysis scoping

The scope definition problem

- What's wrong with these scenarios?
  - Compromise of customer information
  - Database breach
  - Employee commits fraud using customer information

The last two are each subsets of the first one!

The scope drift problem

- You start out measuring one thing, but end up measuring something else. For example:
  - Intended scope:
    - The risk associated with inappropriate access privileges
  - What you actually analyzed:
    - The risk associated with inappropriate insider actions

Avoiding these problems

- Make scoping an explicit part of the analysis process
  - Recognize when there's the potential for double counting/overlap
- When an analysis has been completed, review it to ensure the scope didn't "drift"
  - What you measured = what you intended to measure?

Blind acceptance of tool-generated risk ratings

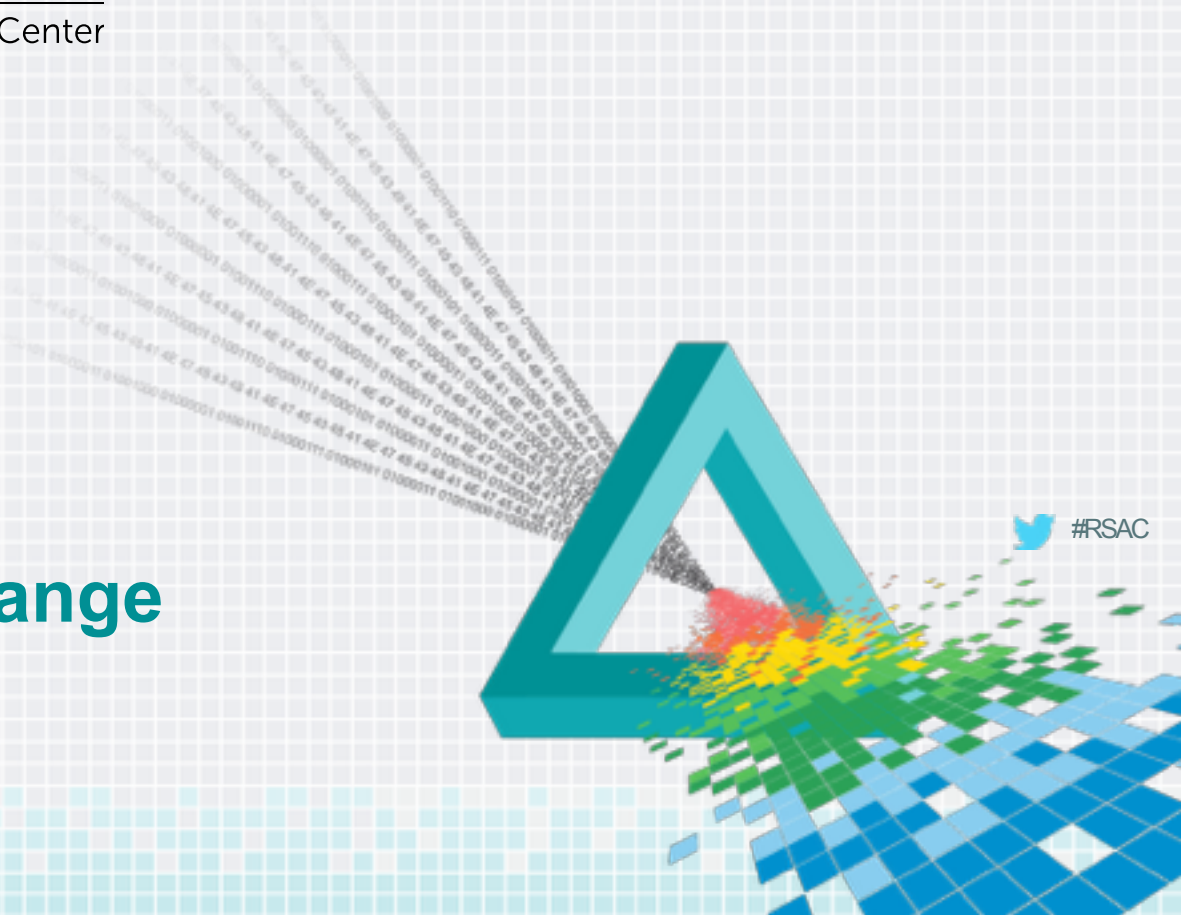
- Scanning and other security technology tools rarely get risk right
  - Leave out key risk elements (e.g., likelihood of an event)
  - Superficially considered factor weights
  - Lots of ordinal math

Avoiding this problem

- Understand the weaknesses in how your tools rate risk
- Apply that understanding and some critical thinking to understand how to adjust/interpret their output

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

The benefits of change

The benefits of change

- Obviously:
  - Improved signal-to-noise ratio
    - Better able to prioritize/focus effectively
      - Fewer opportunities for gaps to occur
      - Reduce wasted resources
- Less obvious:
  - Better credibility and influence with business executives

Applying what we've covered

Apply Slide

- Next week you should:
  - Stop the bleeding — apply more critical thinking to risk ratings
  - Begin pushing back on risk ratings — ask for explanations that stand up
  - Begin recognizing which common problems occur where you work
- In the first three months following this presentation you should:
  - Get calibrated! Read Douglas Hubbard's book
  - Review and clean up your risk register
  - Refine/fix your measurement scales

Apply Slide - continued

- Within six months you should:
  - Fix your models - consider adopting FAIR
  - Improve your ability to scope analyses

Questions?