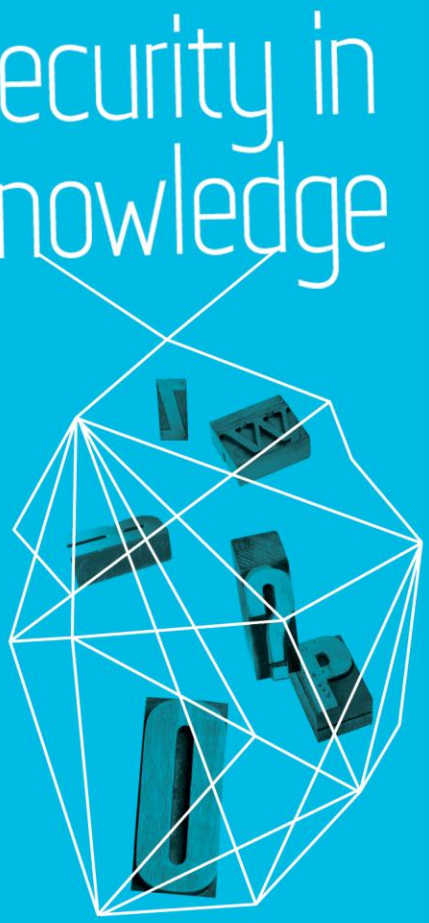
Managing Enterprise Risk: WHY U NO HAZ METRICS?



Moderator:

John D. Johnson
John Deere

Panelists:

Alex Hutton
A Financial Organization

Jack Jones
CXOWARE

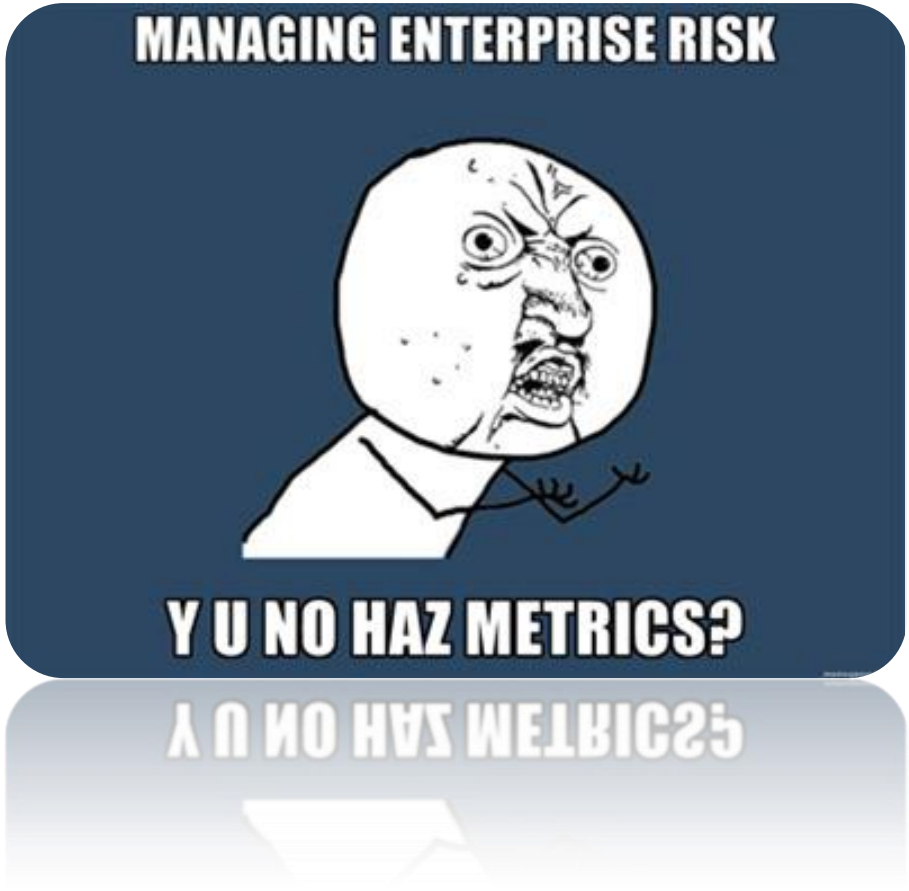
David Mortman
enStratus

Caroline Wong
Symantec

Session ID: GRC-W23

Session Classification: Intermediate

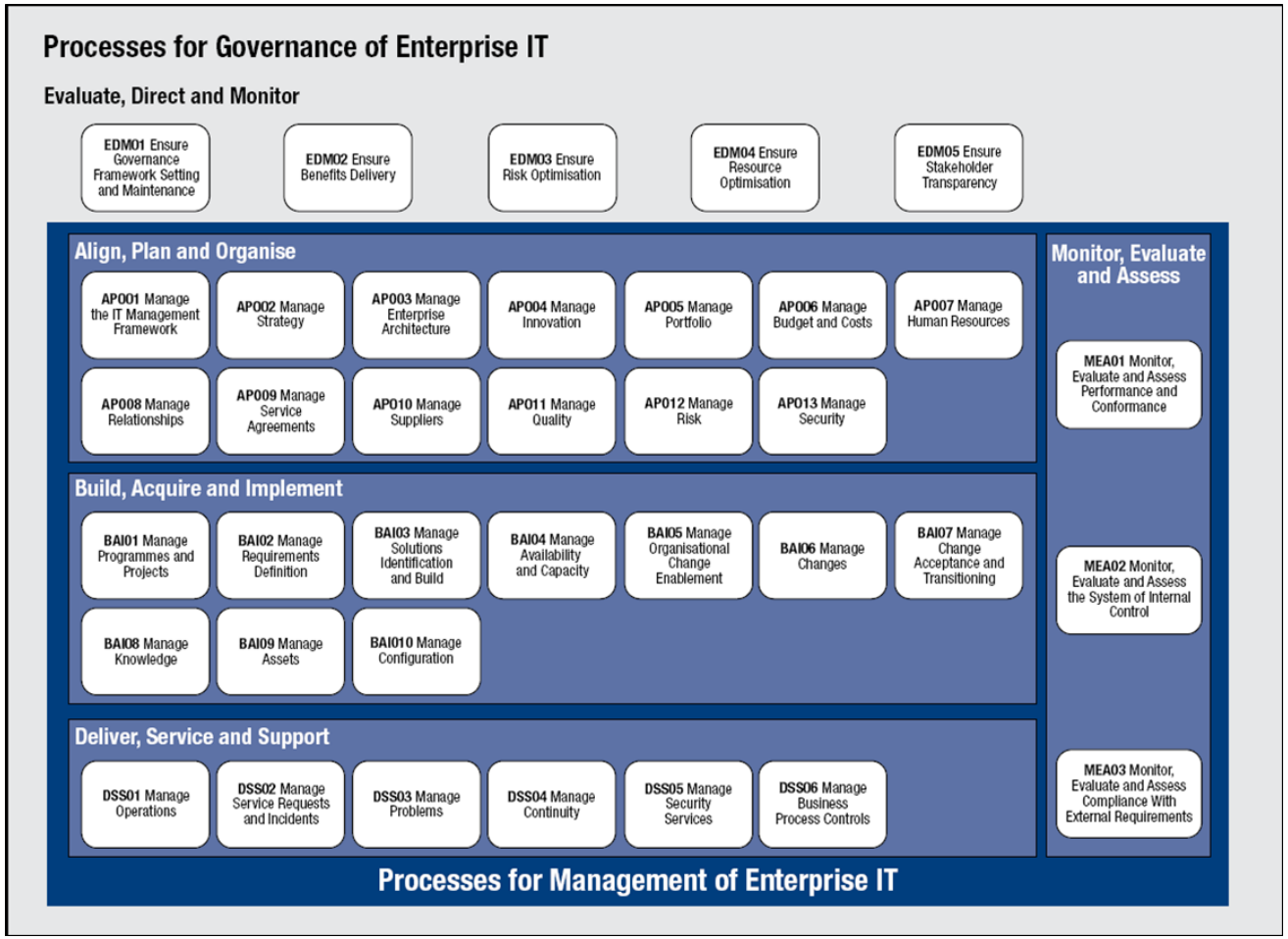
In a nutshell…



Agenda

- How is risk management related to security?
- What is the goal of risk management?
  - How do we define risk?
  - How can we manage risk?
- What is the value of having security metrics?
  - How do I develop meaningful metrics?
- How can good measurements and practices reduce risk?
  - Where can I find models, frameworks & best practices?
    - How can I adapt these for my organization?
  - Are there good data sets I can leverage here?
    - How do I estimate future events by looking at the past? Is this voodoo?

COBIT 5 Process Reference Model

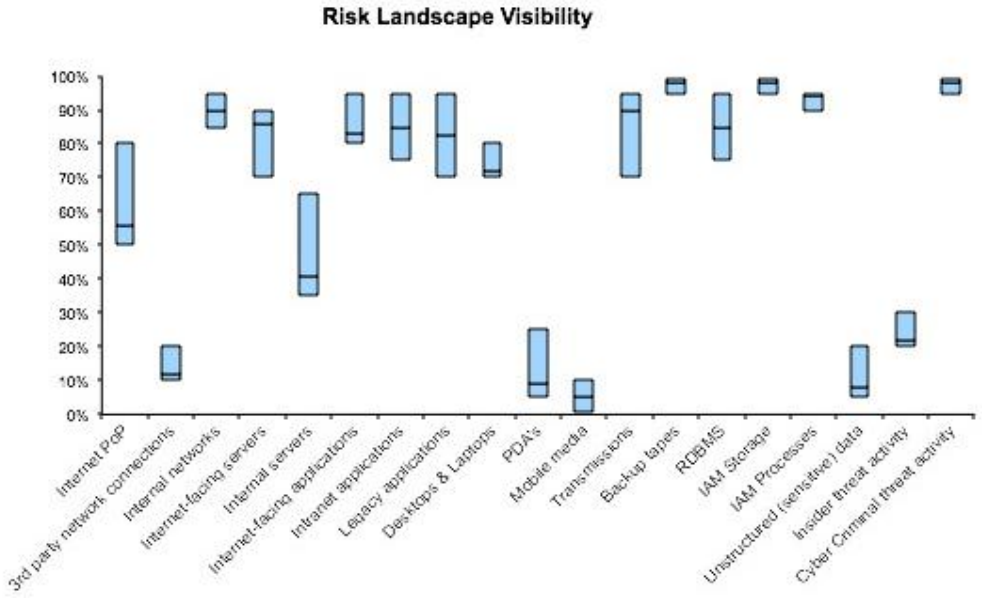


Alex

- Favorites:
  - Cost Center Most At Risk
  - Cost Center With Most Variance
  - Asset Class With Most Variance
- Most Useful:
  - Fraud Cause Counts
  - Amount of Exposure per Cause
  - Amount Lost per Cause

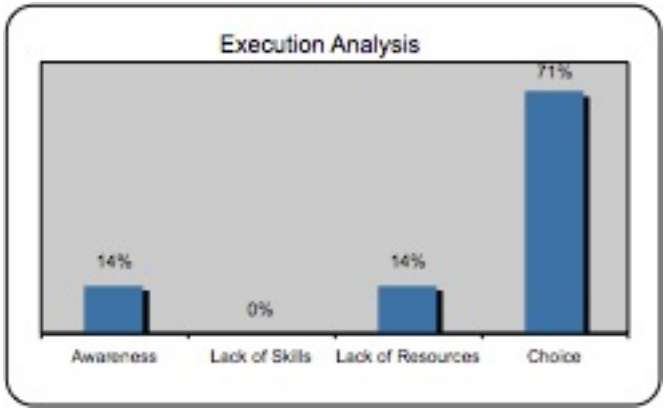
Jack

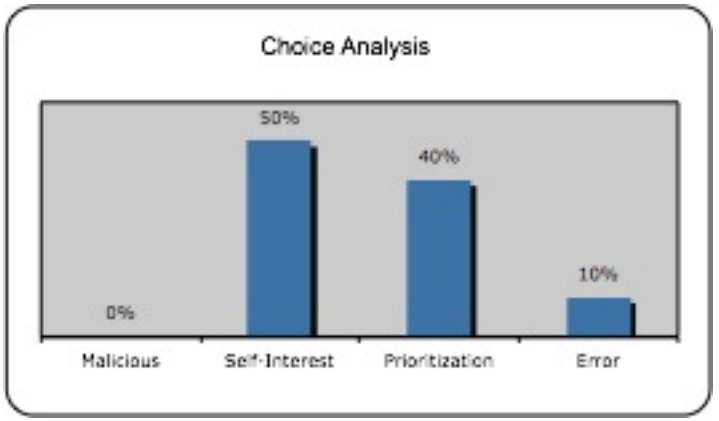
- Risk Landscape Visibility –helps us understand how well informed (or not) our risk decisions are. The values represent data and estimates regarding four elements (asset population, threat conditions, value/liability at risk, and control conditions). This helps us to focus on specific areas of poor visibility, thus improving our ability to make well-informed risk decisions.



Jack

- Root Cause Analysis — which helps us understand why undesirable conditions exist (e.g., non-compliance with policy). This enables us to focus on our efforts to systemically improve.





Caroline: Quantitative and Qualitative Metrics for Patch and Vulnerability Management

Qualitative Metric	Purpose
Which business units receive network vulnerability scan reports from the information security team?	• Visibility for process improvement • Can be used to manage risk and improve performance
Which business units remediate their vulnerabilities based on the scan report	• Visibility for process improvement • Can be used to manage risk and improve performance
Which business units deploy patches within the timeframe specified in the information security group's SLA?	• Visibility for process improvement • Can be used to manage risk and improve performance
Which business units have high-criticality vulnerabilities that have not been remediated in 90 days?	• Visibility for process improvement • Can be used to manage risk and improve performance
Quantitative Metric	**Purpose**
Percentage of patches deployed within the timeframe specified in the information security group's SLA	• Compliance with information security standards and understanding of risk posture
Average time to deploy a normal patch	• Understand risk posture, speed and performance • Can be used to manage performance & decrease avg time
Average time to deploy an emergency patch	• Understand risk posture, speed and performance • Can be used to manage performance & decrease avg time
Comparison of protected areas vs. honeypot areas	• To show results of vulnerability scans, monitoring, logging • Can be used to help measure the benefit of the security program

* Wong, Caroline (2011-10-20). Security Metrics, A Beginner's Guide. McGraw-Hill.

Take Aways

- Security governance needs to mature and be aligned with the business
  - Showing that we can manage enterprise (security) risk will earn us a seat at the table
- Security Governance ≠ GRC
- Governance without metrics & models is voodoo
- Good metrics and practices → Good Governance → Risk Reduction

Take Aways

- "Managing risk means aligning the **capabilities** of the organization, and the **exposure** of the organization with the **tolerance** of the data owners." (Jack)
- "Whatever Metric you present, it is a **risk metric**. Any **security metric** you present will be consciously or sub-consciously **interpreted** by the audience in their own internal risk model. It is inescapable. " (Alex)

Links:

- New School Security Blog
  http://www.newschoolsecurity.com
- FAIR Framework
  http://fairwiki.riskmanagementinsight.com
- Verizon VERIS Framework
  https://verisframework.wiki.zoho.com
- Security Metrics: A Beginner's Guide,
  Caroline Wong
  http://is.gd/6g62uS