tripwire
TAKE CONTROL.

Risky Business 2012: The State of Risk-Based Security Management

Dwayne Melancon, CISA
Chief Technology Officer

Agenda

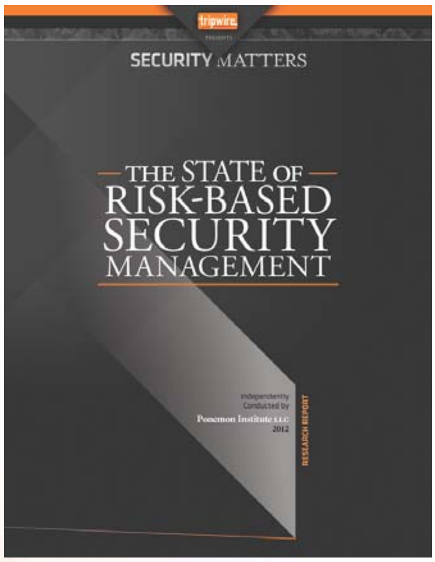
- Overview of the State of Risk Management study
- Discussion of Key Findings
- Field Observations:
  - Effective measurement of security – with an emphasis on effective metrics
  - How are organisations approaching Risk-Based Security Management?

Interest in Risk Management is Spiking

- Increasingly required to engage non-technical executives for budget
- Habitual security spending not aligned with the business
- More objective methods needed to allocate limited budgets
- Scary things in the news, noticed by business guys
- Compliance is driving the conversation around risk

About The State of Risk-Based Security Management Report

- Surveyed 2,145 individuals
- Four countries: US, UK, Germany, Netherlands
- Commissioned by Tripwire
- Conducted by an independent research oranisation, the Ponemon Institute
- ANZ / ASEAN coverage planned for next round of research



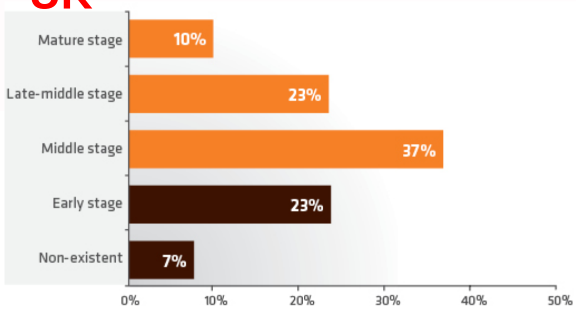
Top Findings

1. More talk than walk
2. Unbalanced approach to information and risk management
3. Lack of metrics to measure success

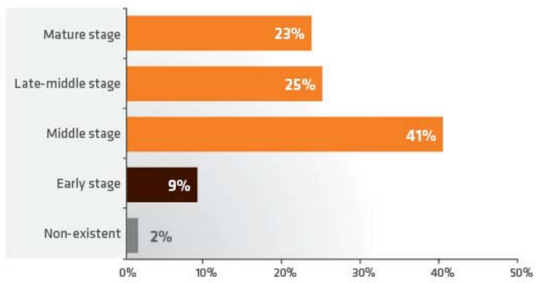
#1 – Lots of Talk. Starting to Walk.

Deployments Range in RBSM Maturity

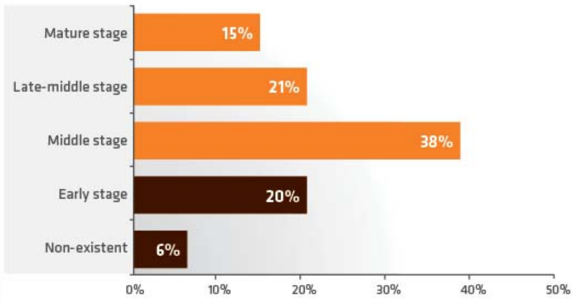
UK



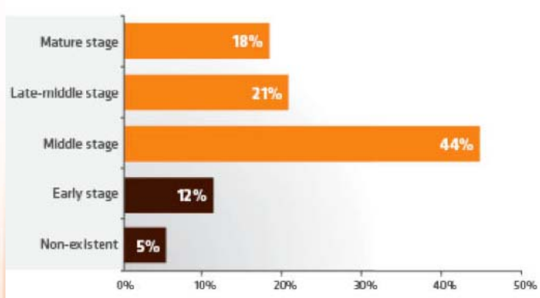
DE



US



NL



Summary: Starting to Walk

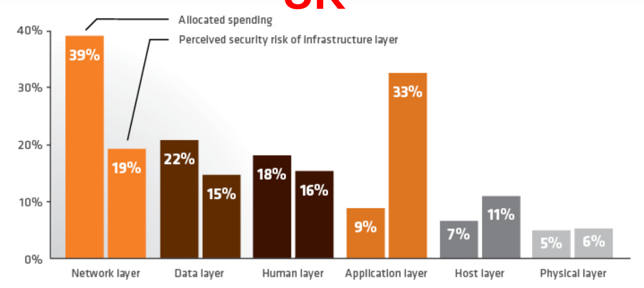
- Most oranisations are talking about risk-based security management
- Most claim to be serious about it
- Less than half have formal strategies or procedures in place

#2 – Unbalanced Approach to Risk & Security

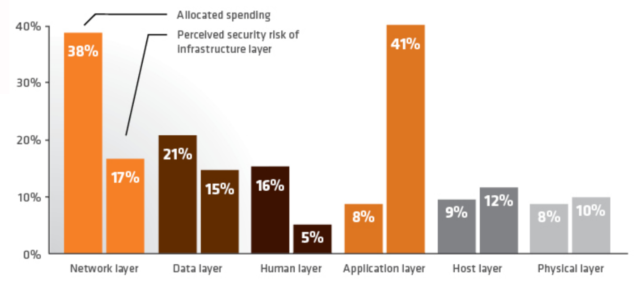
tripwire TAKE CONTROL.

Perceived Risk vs Allocated Spending

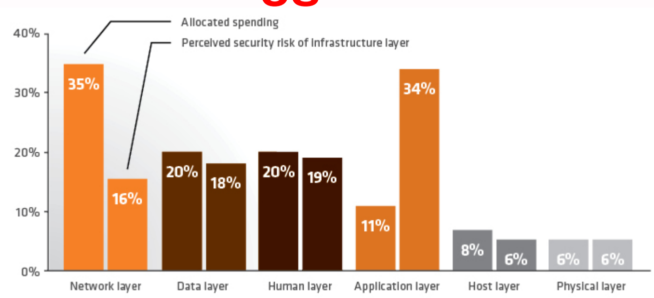
UK



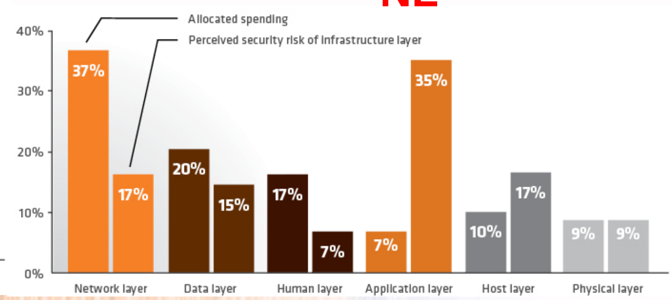
DE



US



NL



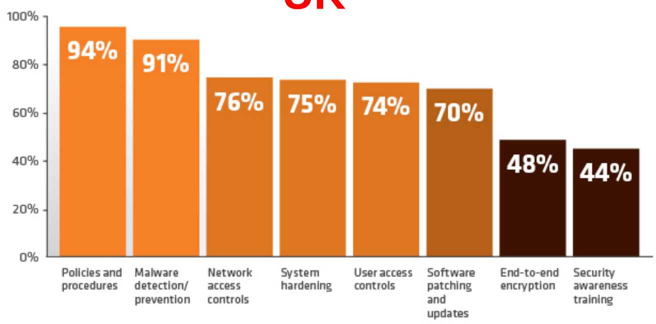
Do the Steps for Assessing and Managing Security Risks Exist?

Basic Steps to Assessing and Managing Security Risk:

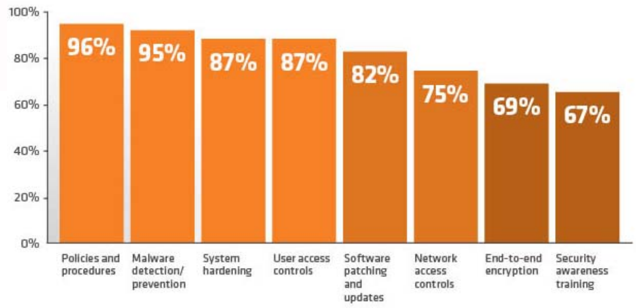
1. Identify the information that is key to the business
2. Categorise information according to its importance to the business
3. Identify threats to the information
4. Assess vulnerabilities to the systems that process the information
5. Assess the risks of loss or corruption of the information
6. Identify controls necessary to mitigate the risks
7. Implement the controls
8. Monitor controls continuously

Existence of Common Preventive Controls

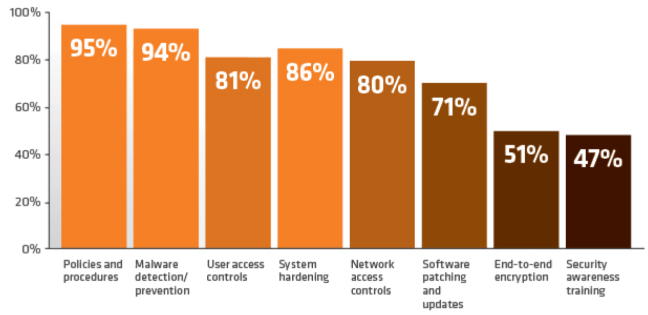
UK



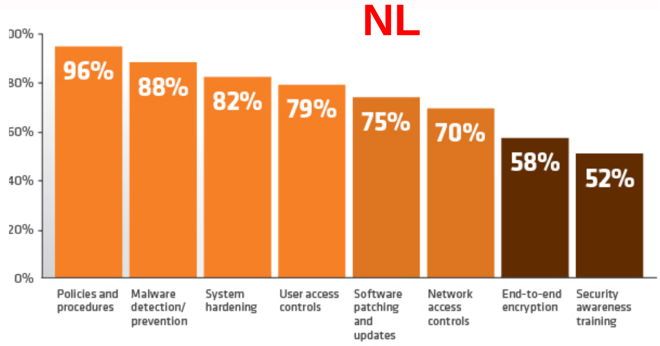
DE



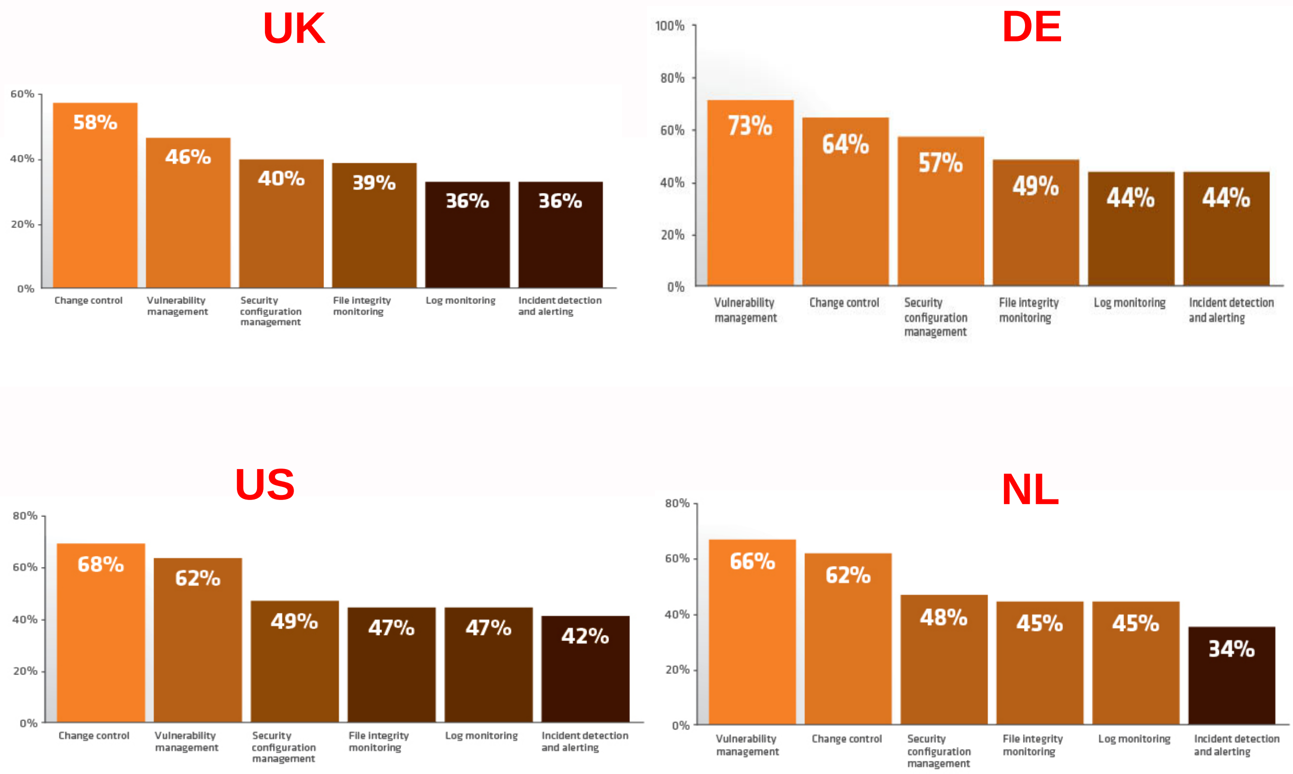
US



NL



Existence of Common Detective Controls



We Have An Opportunity to Improve

Basic Steps to Assessing and Managing Security Risk:

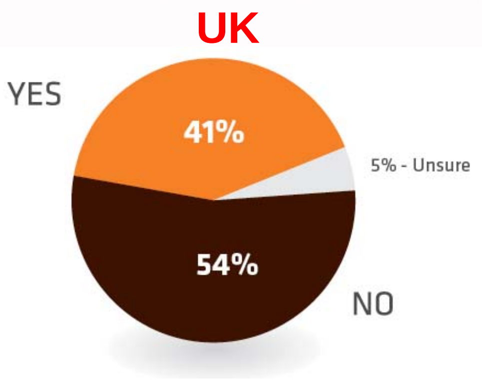
1. Identify the information that is key to the business
2. Categorise information according to its importance to the business
3. Identify threats to the information
4. Assess vulnerabilities to the systems that process the information
5. **Assess the risks of loss or corruption of the information**
6. **Identify controls necessary to mitigate the risks**
7. **Implement the controls**
8. **Monitor controls continuously**

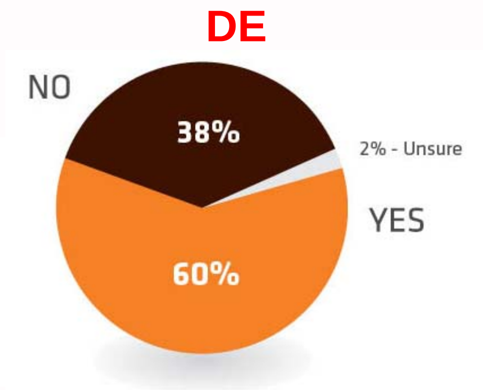
Summary: Unbalanced Approach

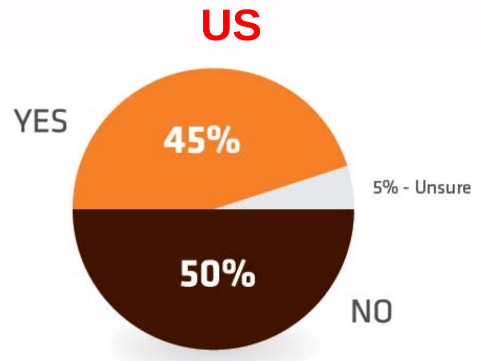
- Security resources are not aligned with the perceived risks
  - Over-investing in some areas, woefully underinvested in others
- Preventive vs. Detective control implementation
  - Oranisations making good progress on preventive controls, yet they are
  - Behind on detective controls; which means
  - They have good expectations, but no way to hold others accountable
- Most have work to do on the critical last steps of RBSM

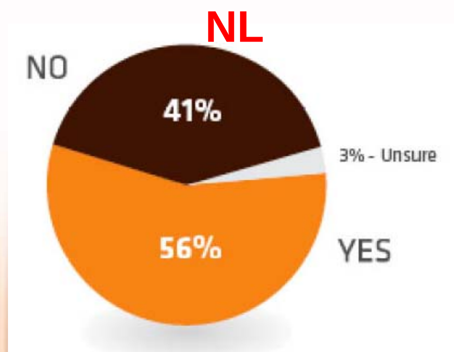
#3 – Lack of Metrics to Measure Success

Use of Metrics to Measure Success



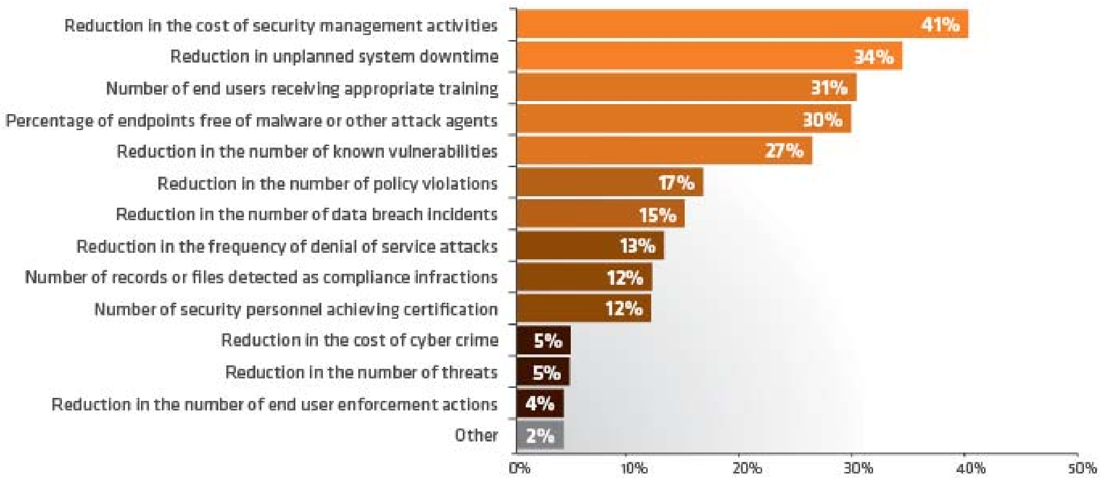






What Is Being Measured?

FIGURE 12. Metrics used to assess effectiveness
More than one response permitted
Source: *The State of Risk-based Security Management: United Kingdom* —©2012 Ponemon Institute, LLC & Tripwire, Inc.



What Is Being Measured?

Summary: Lack of Effective Metrics to Measure Success

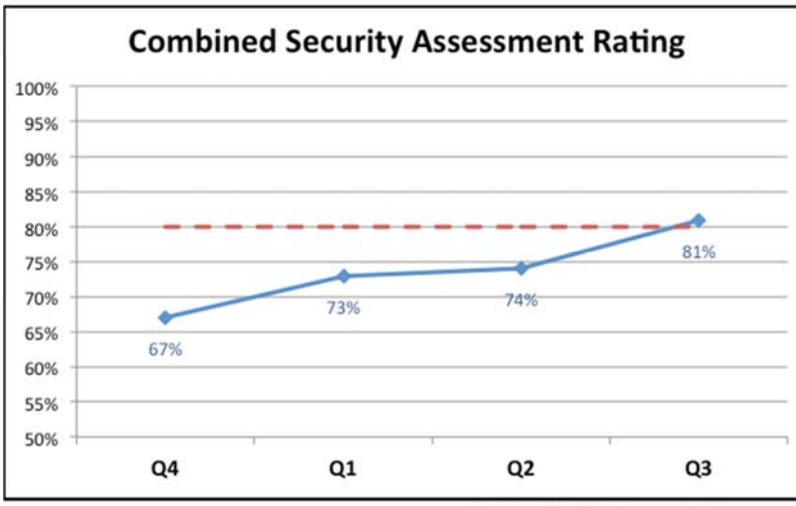
- Less than half of oranisations are using metrics for RBSM
- Many oranisations are using “false flag” metrics
  - Cost of security program
  - Number of vulnerabilities in the environment

Field Observations & Recommendations

Snapshot: Examples Of Metrics That Are Working

- Configuration Quality:
  - % of configurations compliant with target security standards (risk-aligned)
    - i.e. >95% in Critical; >75% in Medium
  - number of unauthorized changes
  - patch compliance by target area based on risk level
    - i.e. % of systems patched within 72 hours for Critical; …within 1 week for Medium
- Control effectiveness:
  - % of incidents detected by an automated control
  - % of incidents resulting in loss
  - mean time to discover security incidents
  - % of changes that follow change process
- Security program progress:
  - % of staff (by business area) completing security training
  - average scores (by business area) for security recall test

Report On Status & Progress vs. Goals



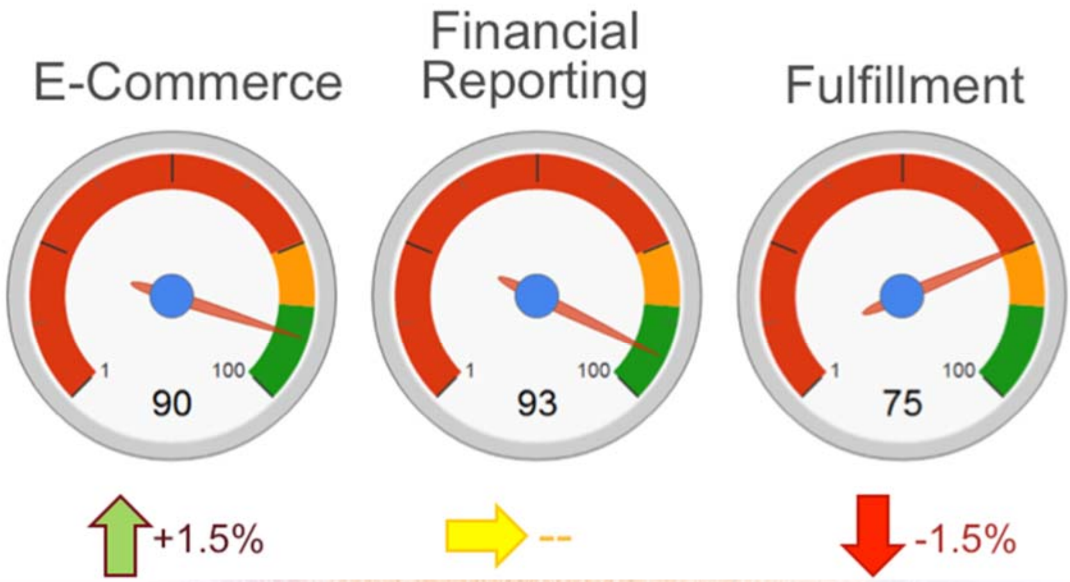
Security Assessment Class	Rating
Change Violations	21%
Anti-Virus Coverage	98%
Configuration Policy	
Authentication	*74%*
Access Controls	*77%*
Services/Ports	*75%*
Log Policies	81%

Filter:

Area	Data Center 2
Policy	NIST 800-53

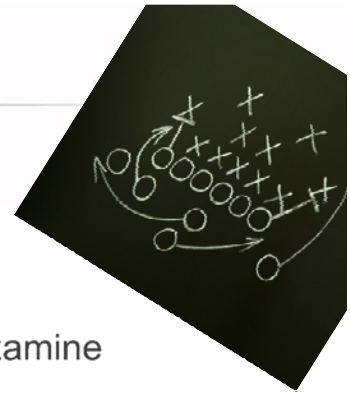
Focus At A Higher Level

Security Status By Business Service
Weekly Summary



IT SECURITY & COMPLIANCE AUTOMATION
@TripwireInc
#RiskyBiz2012
tripwire TAKE CONTROL.

How Are Orgs Approaching RBSM?



- Investigating and adopting a repeatable framework
  - FAIR, OCTAVE, OVAL, CAESARS, ISO, etc.
- Applying risk ranking/scoring methods
- Engaging cross-functional “steering committees” to examine various risks
  - Strategic & Operational, Information Security, Financial, Employment Practices, Intellectual Property, Physical, Legal, Regulatory, etc.
- Prioritizing projects, actions, and investments to bias toward areas of highest risk and impact
- Establishing Key Risk Indicators (KRI’s) and Key Risk Objectives (KRO’s) to measure progress

Don’t Go Overboard

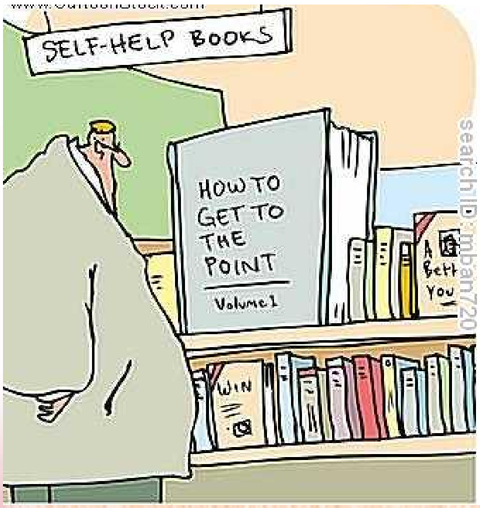


“the Base Equation multiplies **Impact** by 0.6 and **Exploitability** by 0.4”

Jet Engine X Peanut Butter = Shiny

Recommendations: Risk-Based Security Management (RBSM)

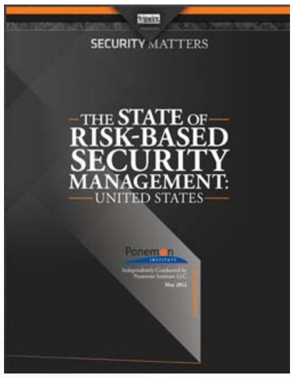
- Institute a formal RBSM program or function with a formal strategy
- Ensure the appropriate balance of preventive and detective controls
- Establish and use metrics to demonstrate program success



Resources

- For your own copy of this study on Risk-Based Security Management
  - www.tripwire.com/ponemon2012
    - Country-specific “slices” of the data are posted
  - Follow @TripwireInc and watch for #RiskyBiz2012

- Keep the conversation going
  - dm@tripwire.com - especially if you have metrics to add to my list
  - Follow me - @ThatDwayne
  - www.tripwire.com/blog



TAKE CONTROL.

www.tripwire.com/ponemon2012
www.tripwire.com/blog
@TripwireInc

Dwayne Melancon
@ThatDwayne

www.tripwire.com
Tripwire Americas: 1.800.TRIPWIRE
Tripwire EMEA: +44 (0) 20 7382 5440
Tripwire Japan: +812.53206.8610
Tripwire Singapore: +65 6733 5051
Tripwire Australia-New Zealand: +61 (0) 402 138 980

@TripwireInc
#RiskyBiz2012