RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: CXO-W02

Security Metrics That Your Board Actually Cares About!

Troy Braban

Chief Information Security Officer
Australia Post
@troybraban

Let's set some ground rules for today.

Aussies have weird accents. Front row: *hands up if I talk too fast*

Audience participation mandatory: *Let's create our own metrics today…*

If you keep doing what you’ve been doing, you’ll keep getting what you’ve been getting.”

- Herrington, J., Bonem, M, & Furr, J

“People who are CISOs in many organizations are excellent technicians…But they don't speak the language of business.”

- Larry Ponemon

83.45%* of metric presentations at 96.82*% of security conferences suck…

* No valid basis for metric. Made up by me

Are we… the security industry… getting this right?

1006

(CIO / CISO / IT: US, Europe, Middle East, Africa)

22%

Board engaged in last 12 months

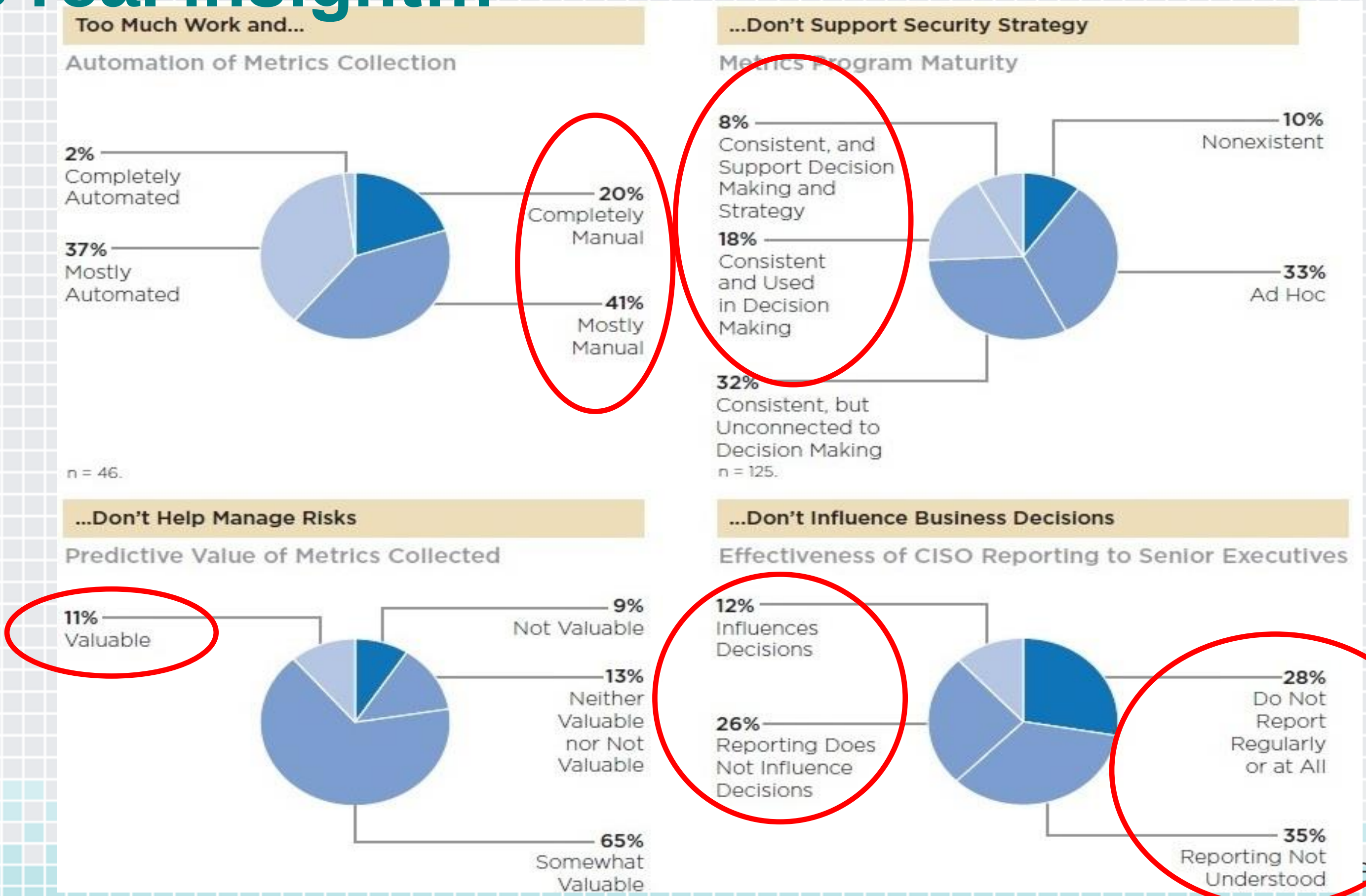
34%

Strategic business priority

Source: Ponemon Institute Global Megatrends CyberSecurity 2015 survey

Our industry has it wrong – compliance is not the way to engage a Board!

A Corporate Executive Board report gives real insight…



Too Much Work and…

Automation of Metrics Collection

…Don't Support Security Strategy

Metrics Program Maturity

…Don't Help Manage Risks

Predictive Value of Metrics Collected

…Don't Influence Business Decisions

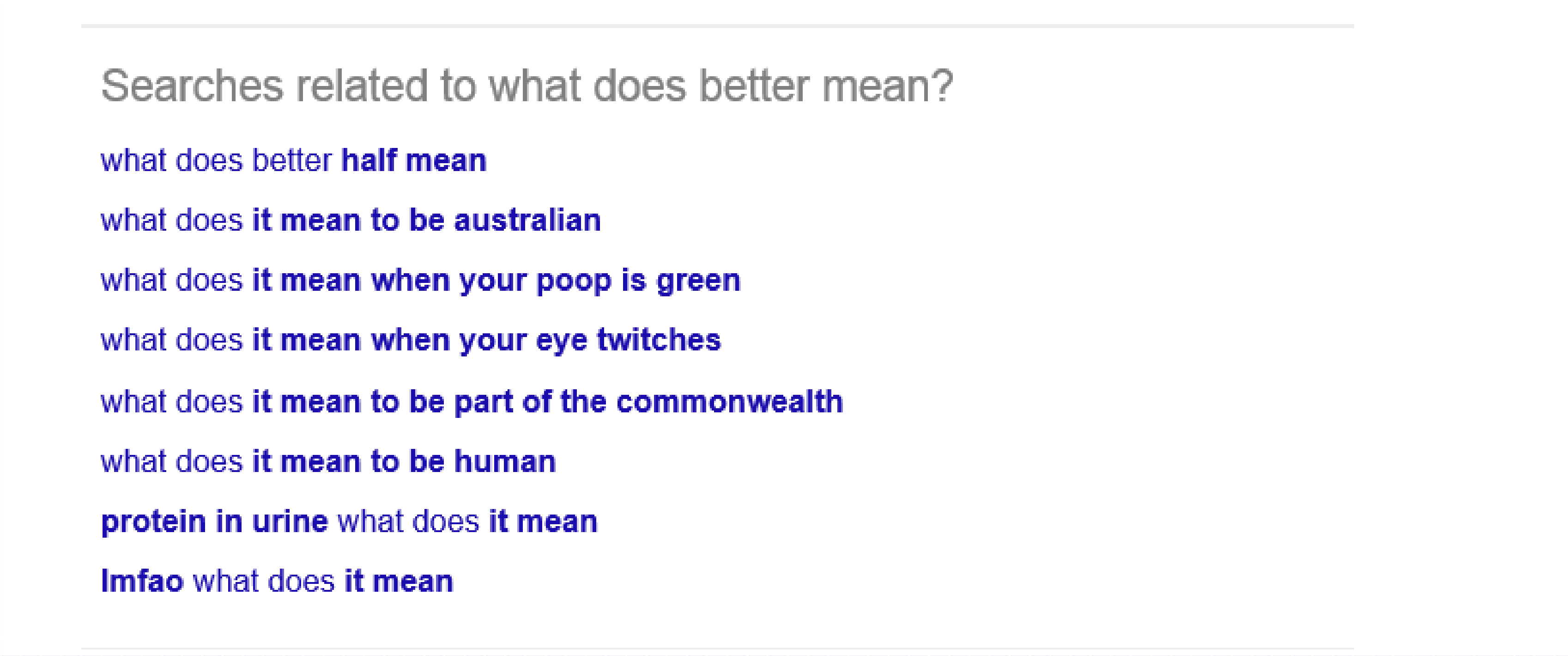
Effectiveness of CISO Reporting to Senior Executives

Source: IREC Information Risk Metrics Report 2011
(used by permission Mia Nomanbhoy, IREC, Jan 13)

…highlighting the need for us to challenge the industry metrics that we use…

- Patch Policy Compliance
- Patch Management Coverage
- Mean-Time to Patch
- Vulnerability Scan Coverage
- Percent of Systems Without Known Severe Vulnerabilities
- Number of Applications
- Percentage of Critical Applications
- Risk Assessment Coverage
- **Security Testing Coverage**
- Mean-Time to Complete Changes
- Percent of Changes with Security Review
- Percent of Changes with Security Exceptions
- **Information Security Budget as % of IT Budget**
- Information Security Budget Allocation
- Mean-Time to Incident Discovery
- Incident Rate
- Percentage of Incidents Detected by Internal Controls
- Mean-Time Between Security Incidents
- Mean-Time to Recovery
- Mean-Time to Mitigate Vulnerabilities
- Number of Known Vulnerability Instances

So… I googled “better”… and it escalated quickly!



Searches related to what does better mean?

what does better **half mean**

what does **it mean to be australian**

what does **it mean when your poop is green**

what does **it mean when your eye twitches**

what does **it mean to be part of the commonwealth**

what does **it mean to be human**

protein in urine what does **it mean**

lmfao what does **it mean**

The “hint” is in what is important for your business…

MyPost Digital Mailbox

World-class parcel network

24/7 Parcel lockers

Australia’s Largest Retail Network

Premium Business Road and Air Delivery

Identity trusted services

24/7 Self-service access

Mobile Applications

Payment Services

Example business scorecard

(NB Not real Australia Post data)

	Measure	Last FY	Target	This FY
Financial	Profit before tax	$823M	$950M	
Strategy	New product take up for existing customer	6.3%	10%	
BU 1	Revenue growth	7.2%	8%	
BU 2	Average revenue per customer	8.6	10	
BU 3	Revenue from new product initiatives	$42.6	$80M	
Product	Product X profitability	15%	18%	
Customer	Net promoter score	+8	+10	
Reputation	Country top 10	6	4	
Employees	Staff engagement	65.8	68	

Example Security Scorecard

(NB Not real Australia Post data)

	Measure	Last FY	Target	This FY
Customer Satisfaction	Customer system downtime caused by IS incident (hours)	15	0	
Reputation	No of IS incidents reported in media	1	0	
Employees	Security staff engagement	74.1%	78%	
Financial	Information security budget as % of IT budget *(Industry average 5%)*	3.5%	4.1%	
Strategy	Information security maturity (0-4) *(industry average 2.2)*	1.8	2.5	
BU 1	No of unmanaged critical or high risk products	5	0	
Brand Protection	Avg time to take down fraudulent websites	52 hrs	36 hrs	

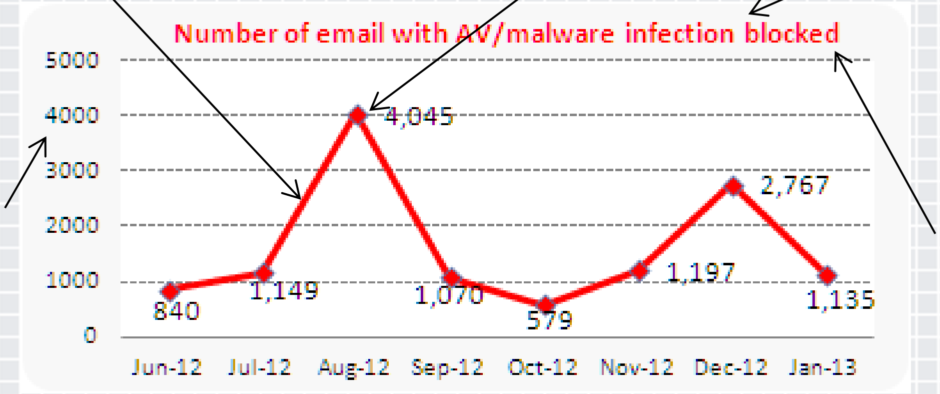
Is this a useful metric?

✓ Shows the trend

? Should we be worried about this peak?

✓ Simple to understand

? Are these numbers high or low? Is this normal?



✗ If it is blocked everything must be ok?

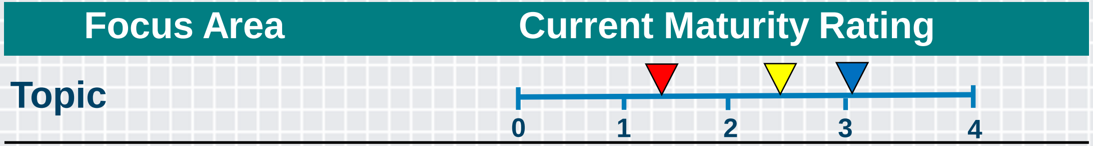
? What decision do you want from me?

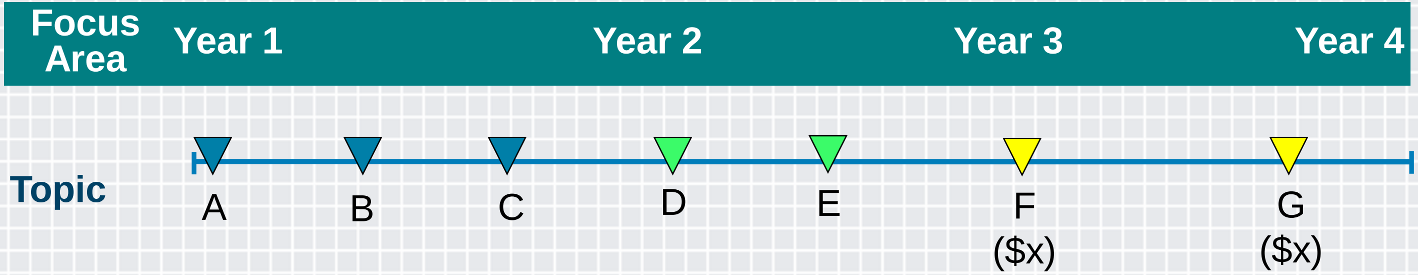
At AP we have taken a different approach. We use a maturity metric model.

Maturity rating is a measure of effectiveness of implemented controls across People, Process & Technology

1 – Compliance Minimum 2 - Industry Baseline
3 - Industry Best Practice 4 - Best in Class

▼ Year 1
▼ Current
▼ Target





To enable our business strategy please approve F and G

▼ Complete ▼ In Budget / Plan ▼ To be funded / scheduled

Just another boring presentation? Or something you'll use?

- When you get back to the office:
  - Throw away your old metrics that aren't leading to decisions
  - Get your business scorecard
  - Work out how security contributes to that scorecard
  - Create your own contribution in business language
  - Repeat…and get better…

- Over time challenge your teams:
  - Can we report on maturity against business need and strategy?
  - What "decisions" have we accepted?
  - What "decisions" does our organisation need to make?