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...

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
- lmfa0 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)

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

(NB Not real Australia Post data)

<table>
<thead>
<tr>
<th>Measure</th>
<th>Last FY</th>
<th>Target</th>
<th>This FY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Satisfaction</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer system downtime caused by IS incident (hours)</td>
<td>15</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>Reputation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of IS incidents reported in media</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>Employees</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security staff engagement</td>
<td>74.1%</td>
<td>78%</td>
<td></td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security budget as % of IT budget <em>(Industry average 5%)</em></td>
<td>3.5%</td>
<td>4.1%</td>
<td></td>
</tr>
<tr>
<td><strong>Strategy</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security maturity (0-4) <em>(industry average 2.2)</em></td>
<td>1.8</td>
<td>2.5</td>
<td></td>
</tr>
<tr>
<td><strong>BU 1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of unmanaged critical or high risk products</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>Brand Protection</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg time to take down fraudulent websites</td>
<td>52 hrs</td>
<td>36 hrs</td>
<td></td>
</tr>
</tbody>
</table>
Is this a useful metric?

- Shows the trend
- Simple to understand
- Should we be worried about this peak?
- Are these numbers high or low? Is this normal?
- If it is blocked everything must be ok?
- What decision do you want from me?

Graph: Number of email with AV/malware infection blocked

- Jun-12: 840
- Jul-12: 1,149
- Aug-12: 1,070
- Sep-12: 579
- Oct-12: 1,197
- Nov-12: 2,767
- Dec-12: 1,135
- Jan-13: 1,135
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

<table>
<thead>
<tr>
<th>Focus Area</th>
<th>Current Maturity Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>0 1 2 3 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Focus Area</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
</tbody>
</table>

($x)$

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?