Measuring Security
How Do I Know What a Valid Metric Looks Like?
Agenda

1. Why measure anything?
2. Good and bad metrics
3. Presenting metrics (visualization)
4. Summary and additional resources
Why Bother?

- **Science**
  - “If you cannot measure it, you cannot improve it.” *Lord Kelvin*
  - “To measure is to know.” *James Clerk Maxwell*

- **Economics**
  - “Measurement motivates.” *John Kenneth Galbraith*

- **Sociology**
  - "Not everything that can be counted counts, and not everything that counts can be counted." *William Bruce Cameron*

- **Consulting**
  - “Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.” *H. James Harrington*
Why Bother?

• Obtain insight
• Speak to the business in its own language
  – The security program has measurable business value
• Objectively demonstrate security objectives are being met
• Justify new investments
• Improve!

"Technical Metrics Aren't Enough: 10 Strategic Security Measures" (Julia Allen & Lisa Young, 2014)
Why Bother?

• The future is coming – can you hear it?

• “Eventually, the insurance industry will subsume the computer security industry.”
  – “Not that insurance companies will start marketing security products, but rather that the kind of firewall you use -- along with the kind of authentication scheme you use, the kind of operating system you use, and the kind of network monitoring scheme you use -- will be strongly influenced by the constraints of insurance.” *Bruce Schneier*

• Will a savvy understanding of the metrics of your internal environment become even more important as this happens?
Poor Metrics

• Easy to collect, but not very actionable
  – Operational metrics ≠ Business-centric metrics

• Examples of what NOT to measure *
  – Spam emails received
  – Virus infection attempts blocked
  – Technical security vulnerabilities resolved
  – Failed logins

• We tend to measure what we can’t control
Poor Metrics

Figure 1. Perimeter Security Incidents (January 2007)

No. of Incidents

- Dropped Packets (x 1,000)
- Detected Intrusions (x 100)
- Viruses Detected (x 1,000)

Source: Gartner (September 2007)

"Toolkit Best Practices: Selecting Security Metrics" (Jeffrey Wheatman/Gartner, 2007)
Poor Metrics

- Subjectively measured
- Inconsistently measured
- Costly to gather
- May not be “metrics” at all
- May not be built for your true audience
Know Your Audience

- Create a common language between the Business and Security
- CISOs are the most influential security-focused consultants to the Business – or rather, they *should* be
- Metrics must reflect the role and the value that the Security organization plays in the Business strategy

Good start. Needs more gibberish.
Know Your Audience

• The “language” of Security is hard for the Business to fully understand
  – Presentation skills are essential – practice!

• Communicating in a Business context
  – Leverage standard templates or communication tools
  – Consider a taxonomy document
Know Your Audience

• Business leaders are extremely busy
  – Connect your message to an identified business driver
  – Critical information should be front and center

• The Business finds it extremely difficult to identify its own risk appetite
  – Consider scenarios and story-telling as tools

• Business leaders are challenged in communicating back to Security, too!
  – Understand the goals/initiatives of the Business units
Abstract Out the Technology & Operational Metrics

• Number of times we were “attacked” last month
• Number of unpatched vulnerabilities
• Number of unpatched critical vulnerabilities against critical systems
• Percentage of unpatched critical vulnerabilities against critical systems
• Number of days it takes to patch critical systems with critical patches
• Number of days it takes to patch systems supporting the manufacturing line in Kuala Lumpur with critical patches
What Makes a “Good” Metric?

- **Actionable**: The source of the problem, or necessary actions to take, are clear when the metric goes up, down, flat or off-target.
- **Common interpretation**: People in the organization recognize what the metric means.
- **Accessible, creditable data**: The data can be acquired with modest effort from a source that people trust.
- **Transparent, simple calculation**: How the metric is generated is shared and easy to understand.

The perfect metric

"Choosing the Right Metric" (Zach Gemignani, 2007) [http://www.juiceanalytics.com/writing/choosing-right-metric]
What Makes a “Good” Metric?

• “The primary goal of metrics is to quantify data to facilitate insight.” Andrew Jaquith

• A good metric is:
  – Consistently measured
  – Cheap to gather
  – Expressed as cardinal number or percentage
  – Expressed using at least one unit of measure
  – Contextually specific
What Makes a “Good” Metric?

- Quantifiable information
  - Ability to compare and trend
- Readily obtainable
- Consistent and repeatable processes only
- Track relevant performance trends over time
- Point to improvement actions
What Makes a “Good” Metric?

- Avoids measuring non-events
- Clarifies ownership of key assets
- Knows its audience
Five Security Metrics to Consider
Abstract Out the Technology & Operational Metrics

- Number of times we were “attacked” last month
- Number of unpatched vulnerabilities
- Number of unpatched critical vulnerabilities against critical systems
- Percentage of unpatched critical vulnerabilities against critical systems
- Number of days it takes to patch critical systems with critical patches
- Number of days it takes to patch systems supporting the manufacturing line in Kuala Lumpur with critical patches
Five Security Metrics to Consider

1. Time elapsed between incident discovery and incident containment

Be thinking about...

- Are you equipped to measure this, or are you just putting out fires?
- Do you have an incident tracking system in place today?
- Have you explicitly defined what “containment” means?
- Do you also track/report on root cause as part of your process?
Five Security Metrics to Consider

2. Number of orphaned information assets without an owner

Be thinking about...

• Do you know where all of your information assets reside?
• Do you explicitly assign/name owners for assets? How does this process work today?
• Do all of your information assets need an owner?
• How do you know if a designated/responsible owner is still on the payroll?
Five Security Metrics to Consider

3. Days to remediate 50% (the “half-life”) of vulnerable hosts

Be thinking about...

- Do you prioritize vulnerability remediation based on asset criticality?
- Should you differentiate between internal & external systems?
- What is your exception/escalation process for critical assets, if any?
Five Security Metrics to Consider

4. Number of server patches applied outside of a scheduled maintenance window

Be thinking about...

- Do you have established maintenance windows?
- Are your maintenance windows consistent across server platforms? Should they be?
- What criteria determines when a patch should be pushed?
- Are you classifying (and scoring) vulnerabilities as part of this exercise?
Five Security Metrics to Consider

5. Percentage of third-party users whose privileges were reviewed this reporting period

Be thinking about...

• Do you understand your potential third-party vendor areas of risk?
• Do you know which external vendors have accounts associated with your assets?
• Are there any assets where electronic communication to/from external vendors (including system-to-system access) is simply not allowed?
Five Security Metrics to Consider

1. Time elapsed between incident discovery and incident containment
2. Number of orphaned information assets without an owner
3. Days to remediate 50% (the “half-life”) of vulnerable hosts
4. Number of server patches applied outside of a scheduled maintenance window
5. Percentage of third-party users whose privileges were reviewed this reporting period
Caveats

• Don’t blindly accept your vendor’s proffered metrics.
  – “We tend to overvalue the things we can measure and undervalue the things we cannot.” John Hayes

• Metrics should be actionable!
  – “If a measurement matters at all, it is because it must have some conceivable effect on decisions and behaviour. If we can't identify a decision that could be affected by a proposed measurement and how it could change those decisions, then the measurement simply has no value.” Douglas W. Hubbard
Is there only one interpretation?

"More than Mitigating Risk: The Future of Co-Creating Value with Stakeholders" (Tara Addis, 2011)

Visualization

Ben Smith @Ben_Smith · Jun 2
When done right, data visualization is the perfect marriage between art and information. #dataviz
Visualization

<table>
<thead>
<tr>
<th></th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>10.0</td>
<td>10.0</td>
<td>10.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>8.04</td>
<td>9.14</td>
<td>7.46</td>
<td>6.58</td>
</tr>
<tr>
<td>x</td>
<td>8.0</td>
<td>8.14</td>
<td>8.0</td>
<td>6.77</td>
</tr>
<tr>
<td>y</td>
<td>6.95</td>
<td>8.14</td>
<td>6.77</td>
<td>5.76</td>
</tr>
<tr>
<td>x</td>
<td>13.0</td>
<td>13.0</td>
<td>13.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>7.58</td>
<td>8.74</td>
<td>12.74</td>
<td>7.71</td>
</tr>
<tr>
<td>x</td>
<td>9.0</td>
<td>9.0</td>
<td>9.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>8.81</td>
<td>8.77</td>
<td>7.11</td>
<td>8.44</td>
</tr>
<tr>
<td>x</td>
<td>11.0</td>
<td>11.0</td>
<td>11.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>8.33</td>
<td>9.26</td>
<td>7.81</td>
<td>8.47</td>
</tr>
<tr>
<td>x</td>
<td>14.0</td>
<td>14.0</td>
<td>14.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>9.96</td>
<td>8.10</td>
<td>8.84</td>
<td>7.04</td>
</tr>
<tr>
<td>x</td>
<td>6.0</td>
<td>6.0</td>
<td>6.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>7.24</td>
<td>6.13</td>
<td>6.08</td>
<td>5.25</td>
</tr>
<tr>
<td>x</td>
<td>4.0</td>
<td>4.0</td>
<td>4.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>4.26</td>
<td>3.10</td>
<td>5.39</td>
<td>5.25</td>
</tr>
<tr>
<td>x</td>
<td>12.0</td>
<td>12.0</td>
<td>12.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>10.84</td>
<td>9.13</td>
<td>8.15</td>
<td>5.56</td>
</tr>
<tr>
<td>x</td>
<td>7.0</td>
<td>7.0</td>
<td>7.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>4.82</td>
<td>7.26</td>
<td>6.42</td>
<td>7.91</td>
</tr>
<tr>
<td>x</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
<td>8.0</td>
</tr>
<tr>
<td>y</td>
<td>5.68</td>
<td>4.74</td>
<td>5.73</td>
<td>6.89</td>
</tr>
</tbody>
</table>

"Anscombe's quartet" [https://en.wikipedia.org/wiki/Anscombe%27s_quartet]
Visualization vs. Textual Analysis of Data

• Answers a question
• Poses new questions
• Explore and discover
• Communicate information
• Increase efficiency
• Be inspired!
Edward Tufte

• Five guidelines for data graphics
  – Above all else, show the data!
  – Maximize data-to-ink ratio
  – Erase non-data ink
  – Erase redundant data ink
  – Revise and edit

• Avoid “chartjunk”
Some of Tufte’s Greatest Hits

• “The single biggest threat to the credibility of a presentation is cherry-picked data.”

• “When watching a presentation, ask yourself: ‘Am I seeing the result of information or information selection?’”

• “Clutter and confusion are failures of design, not attributes of information.”

• “If the numbers are boring, then you've got the wrong numbers.”
Pie Charts: the Holy War

• When is it time for pie?
  – Low number (≤6) of variables
  – Pie must represent a meaningful total
  – Large disparity between values
  – As a check, ask yourself:
    • Why not a bar chart? Or a table?

• Agree?
  – “Save the Pies for Dessert” (Stephen Few, 2007)

• Disagree?
  – "Why Tufte is Flat-Out Wrong about Pie Charts" (Bruce Gabrielle, 2013)
    http://speakingppt.com/2013/03/18/why-tufte-is-flat-out-wrong-about-pie-charts/
Final Thought: the “Data Cake”

The one place to start for a foundational background (strategic)

Or, skip to here for content specific to information security (tactical)
More on Metrics & Visualization

• Online resources
  – Mailing lists
    • Security Metrics  http://www.securitymetrics.org/mailing-list.html
    • Society of Information Risk Analysts  http://lists.societyinforisk.org/mailman/listinfo/sira
  – Proceedings
    • Metricon  http://www.securitymetrics.org/
    • Visualization for Cyber Security (VizSec)  http://www.vizsec.org/
  – Frameworks / References
    • ISO 27004 ($$): “Information technology - Security techniques - Information security management – Measurement”

• Key readings (appendices to this presentation)
  – Additional freely-available online resources
  – Subscription-based ($$) analyst collateral
Appendix: Additional Online Resources

- “Lord Kelvin Was Wrong” (Ben Tomhave, 2011) http://www.secureconsulting.net/2011/03/lord-kelvin-was-wrong.html
- "Measuring Security” (Dan Geer, 2007) http://all.net/Metricon/measuringsecurity_tutorial.pdf
- “Choosing the Right Metric” (Zach Gemignani, 2007) http://www.juiceanalytics.com/writing/choosing-right-metric
Appendix: Additional Online Resources

• Metrics

• Visualization
Appendix: Analyst Reports

- Gartner
  - “Sharpen Your Security Metrics to Make Them Relevant and Effective” (Rob McMillan, 2014) [G00259303]
  - “Five Required Characteristics of Security Metrics” (Rob McMillan, 2012) [G00245748]
  - “From Practitioners to Management: Getting Real About Security Metrics” (Ramon Krikken, 2012) [G00226260]
  - “How to Run, Grow, and Transform Your Risk and Security Program” (Paul Proctor, 2012) [slides]
  - “Ten Reasons Security Is Overlooked in Information Governance, and How to Fix It” (Jeffrey Wheatman, 2011) [G00226989]
  - “Five Required Characteristics of Security Metrics” (Jeffrey Wheatman, 2011) [G00212728]
  - “Developing Key Risk Indicators - The Relationship Between KRIs and KPIs” (Paul Proctor, 2010) [G00209075]
  - “Eight Practical Tips to Link Risk and Security to Corporate Performance” (Paul Proctor, 2010) [G00173779]

These reports are only available through a paid subscription to the analyst firm.
Appendix: Analyst Reports

• Gartner
  – “Security and Risk Management as a Social Science” (Tom Scholtz, 2010) [G00206145]
  – “How to Close the Gap Between Information Security and IT Risk Management” (Jeffrey Wheatman, 2009) [G00171144]
  – “How to Move Beyond Security Awareness to Create a Risk-Conscious Culture” (Jay Heiser, 2008) [G00156433]
  – “Improve the Impact of Security Awareness Training by Aligning Metrics and Training Design” (Andrew Walls, 2008) [G00161716]
  – “The Do's and Don'ts of Information Security Metrics” (Jeffrey Wheatman, 2008) [G00162191]
  – “A Simple Method for Expressing Information Criticality and Classification” (Jay Heiser, 2008) [G00155346]
  – “Measure the Effectiveness of Your Security Awareness Training Program” (Ray Wagner, 2005) [G00125684]
  – “Security Metrics - Horses for Courses” (Fred Cohen, 2005) [G00203126]
  – “Justify Identity Management Investment With Metrics” (Roberta Witty, 2004) [TG-22-1617]

These reports are only available through a paid subscription to the analyst firm.
Appendix: Analyst Reports

- Forrester
  - “Determine The Value Of Information Security Assets And Liabilities — Information Security Economics 102” (Ed Ferrara, 2013) [94861]
  - “Measure The Effectiveness Of Your Security Architecture And Operations” (Ed Ferrara, 2012) [83501]
  - “Develop Effective Security Metrics” (Ed Ferrara, 2012) [45787]
  - “The Forrester Information Security Metrics Maturity Model” (Ed Ferrara, 2012) [61232]
  - “How to Market Security To Gain Influence And Secure Budget” (Jinan Budge, 2011) [58010]
  - “Don’t Bore Your Executives - Speak To Them In A Language That They Understand” (Ed Ferrara, 2011) [58885]
  - “Case Study - Verizon Business Builds An Asset-Based Security Metrics Program” (Khalid Kark, 2008) [46346]
  - “Best Practices: Security Metrics” (Khalid Kark, 2008) [45787]

These reports are only available through a paid subscription to the analyst firm.
Appendix: Analyst Reports

- **Forrester**
  - “Defining An Effective Security Metrics Program” (Khalid Kark & Paul Stamp, 2007) [42354]
  - “Defining An Information Security Metrics Framework” (Khalid Kark, 2006) [slides]
  - “Anatomy Of An IT Balanced Scorecard Project” (Craig Symons, 2006) [39665]
  - “Are We Secure Yet?” (Khalid Kark, 2006) [39168]
  - “Bridging The Security Divide” (Paul Stamp, 2006) [36280]
  - “How to Measure What Matters In Security” (Laura Koetzle, 2006) [38640]
  - “The Myths Of Information Security Reporting” (Khalid Kark, 2006) [39148]
  - “Measuring The Business Value Of IT” (Craig Symons, 2006) [40267]
  - “The Marketing Of IT” (Laurie Orlov, 2005) [37384]
  - “Policies Should Support Business Requirements And Establish Metrics” (Michael Rasmussen, 2004) [35300]

*These reports are only available through a paid subscription to the analyst firm.*