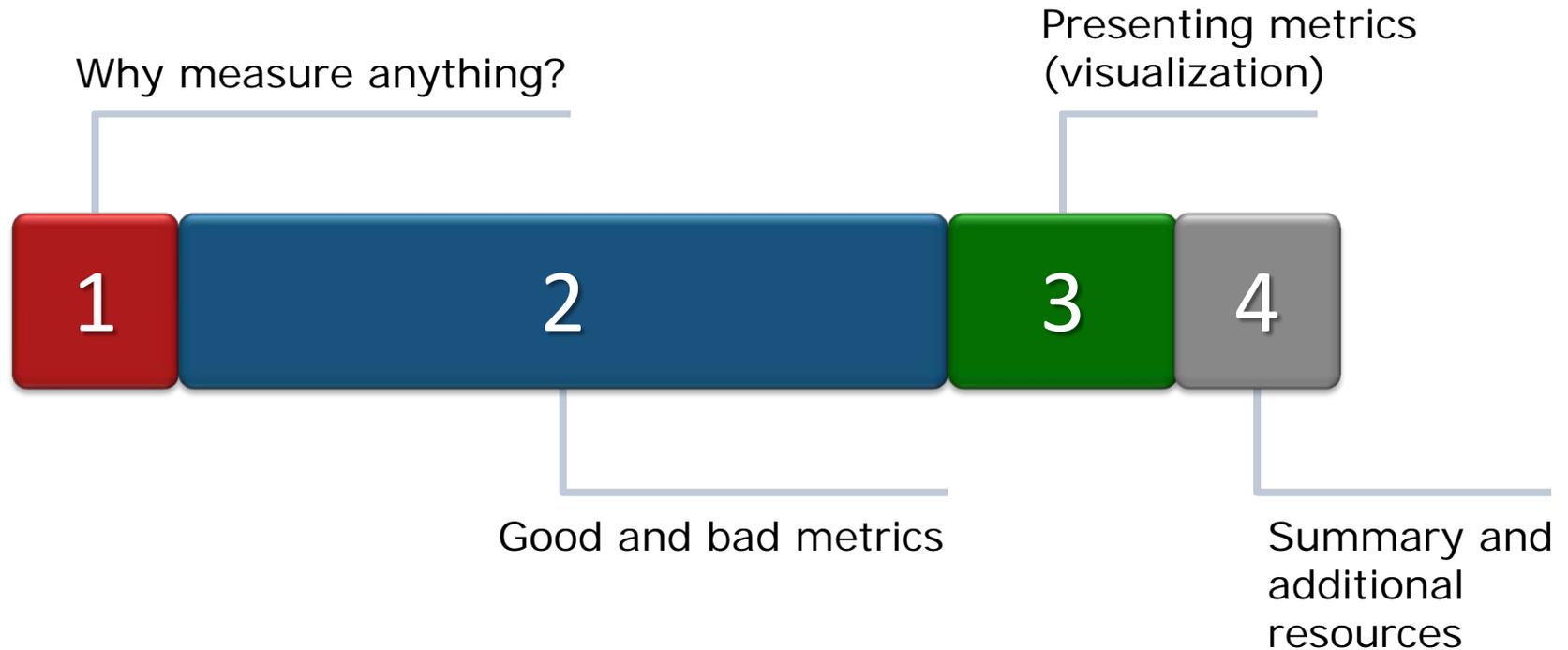




Measuring Security

How Do I Know What a Valid Metric Looks Like?

Agenda



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!

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?

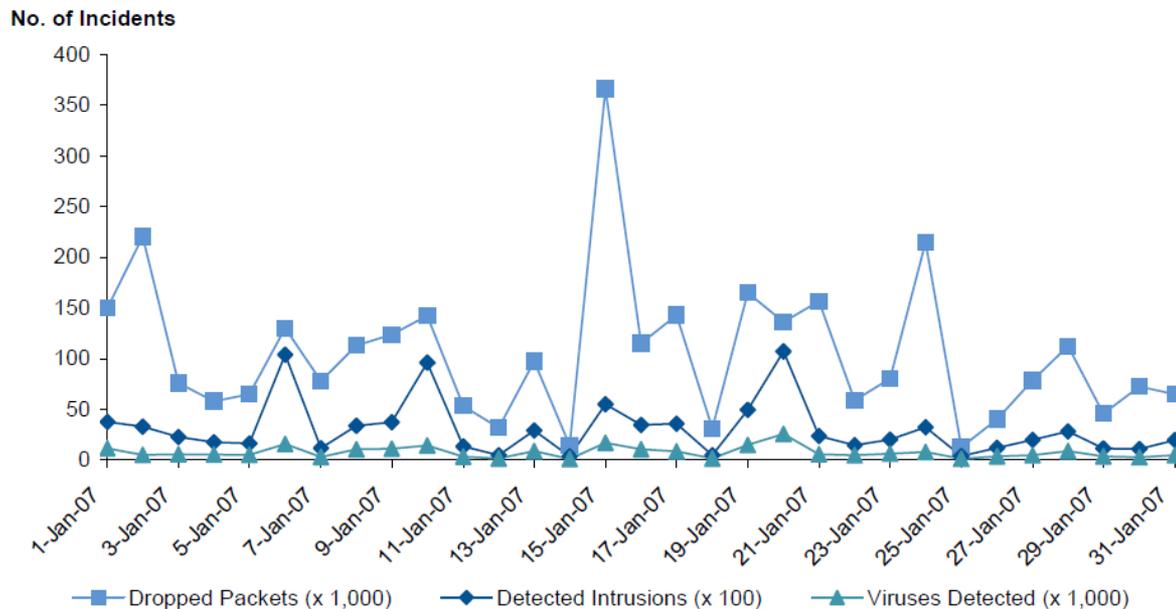


Poor Metrics

- Easy to collect, but not very actionable
 - Operational metrics \neq 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)



Source: Gartner (September 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



Good start. Needs more gibberish.

- 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

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?

The source of the problem, or necessary actions to take, are clear when the metric goes up, down, flat or off-target

People in the organization recognize what the metric means

The perfect metric →

Actionable

Common interpretation

Accessible, creditable data

Transparent, simple calculation

The data can be acquired with modest effort from a source that people trust

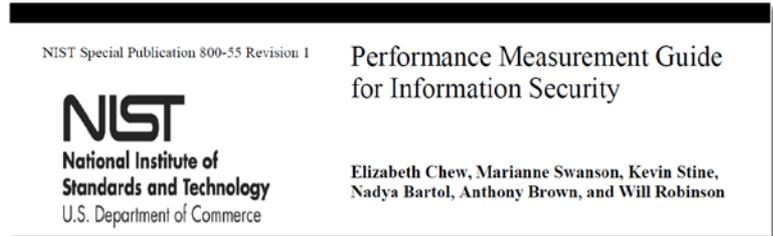
How the metric is generated is shared and easy to understand

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

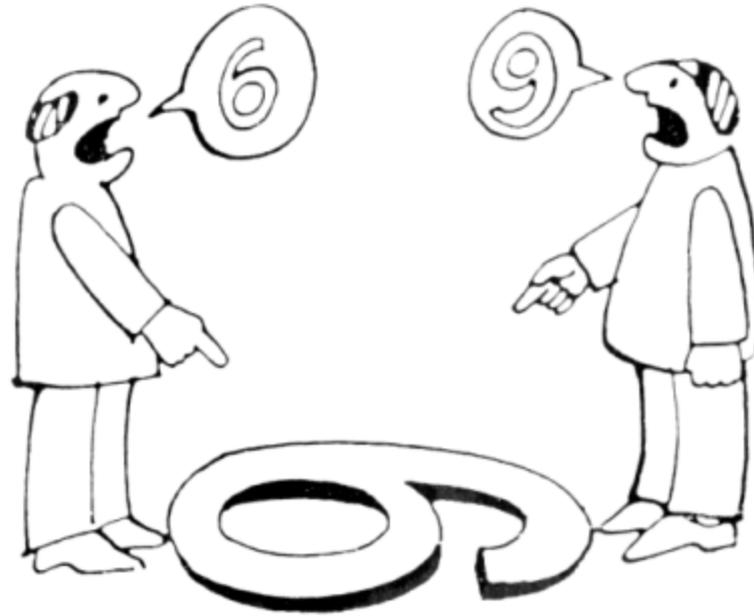
1. Time elapsed between incident discovery and incident containment
2. Number of orphaned information assets without an owner
3. Days to remediate 50% (the "half-life") of vulnerable hosts
4. Number of server patches applied outside of a scheduled maintenance window
5. Percentage of third-party users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

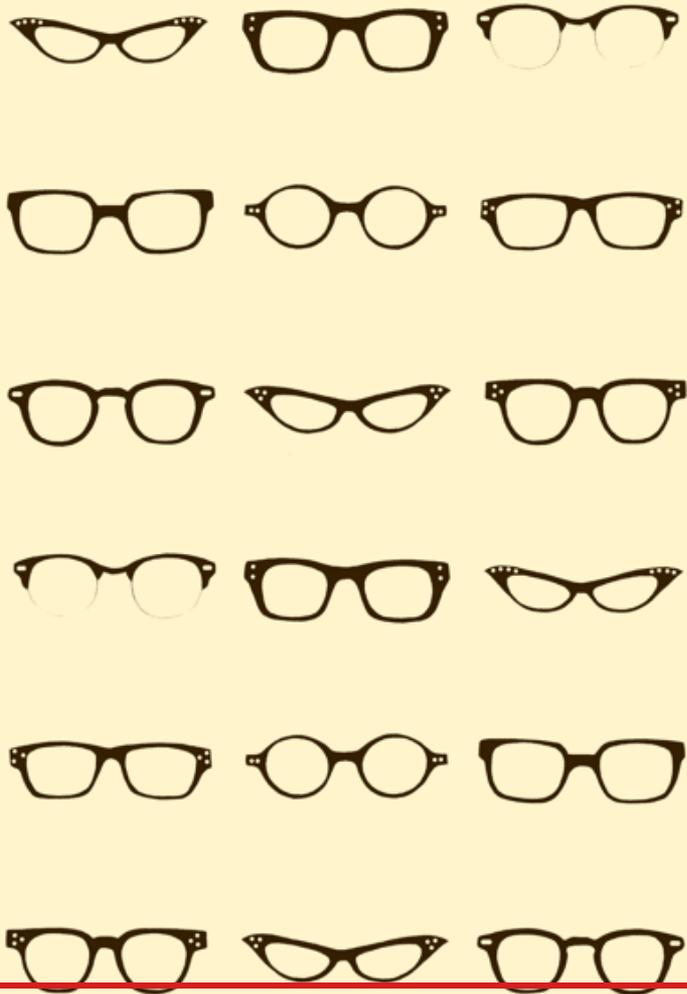


Caveats

- 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?





Visualization



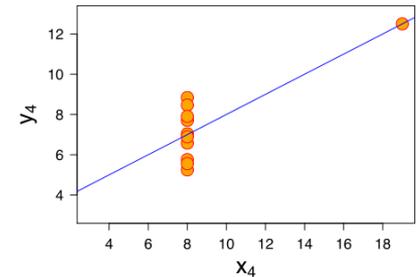
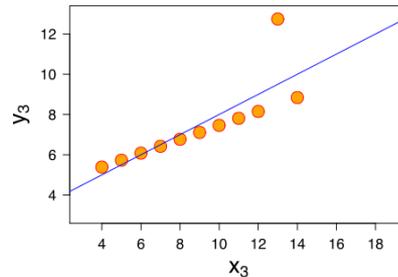
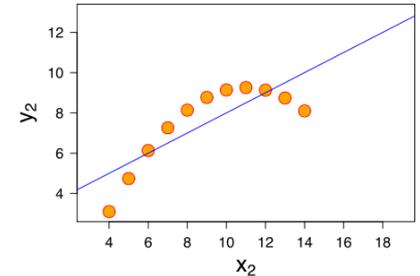
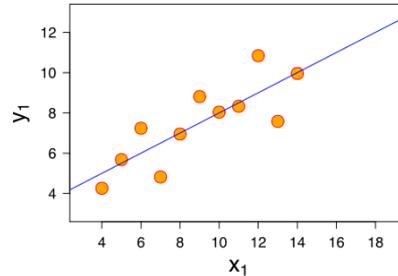
Ben Smith @Ben_Smith · Jun 2

When done right, data visualization is the perfect marriage between art and information. #dataviz



Visualization

I		II		III		IV	
x	y	x	y	x	y	x	y
10.0	8.04	10.0	9.14	10.0	7.46	8.0	6.58
8.0	6.95	8.0	8.14	8.0	6.77	8.0	5.76
13.0	7.58	13.0	8.74	13.0	12.74	8.0	7.71
9.0	8.81	9.0	8.77	9.0	7.11	8.0	8.84
11.0	8.33	11.0	9.26	11.0	7.81	8.0	8.47
14.0	9.96	14.0	8.10	14.0	8.84	8.0	7.04
6.0	7.24	6.0	6.13	6.0	6.08	8.0	5.25
4.0	4.26	4.0	3.10	4.0	5.39	19.0	12.50
12.0	10.84	12.0	9.13	12.0	8.15	8.0	5.56
7.0	4.82	7.0	7.26	7.0	6.42	8.0	7.91
5.0	5.68	5.0	4.74	5.0	5.73	8.0	6.89



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.”

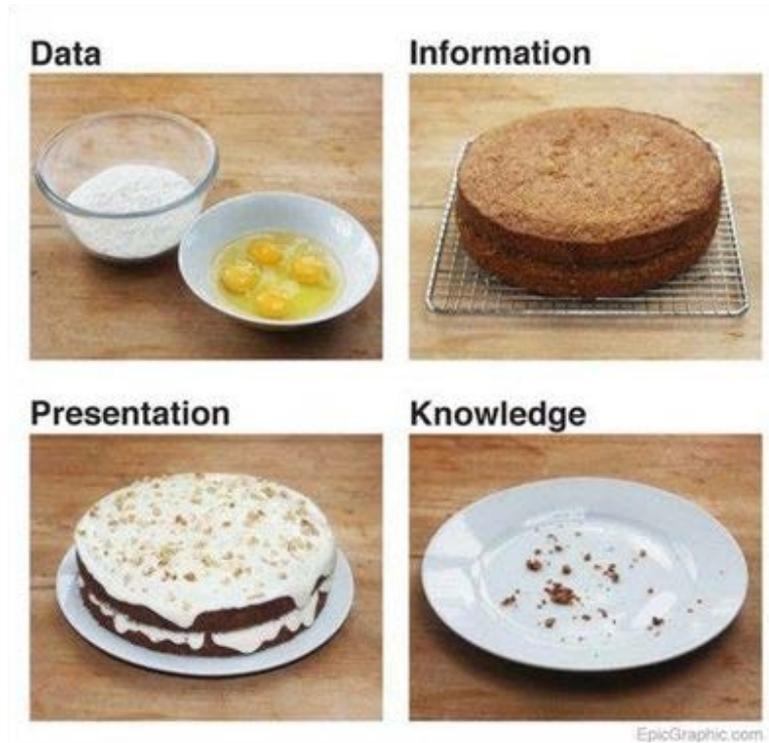
Pie Charts: the Holy War

- 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)
http://www.perceptualedge.com/articles/visual_business_intelligence/save_the_pies_for_dessert.pdf
- 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/>

World's Most Accurate Pie Chart



Final Thought: the "Data Cake"

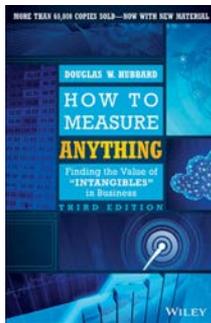


More on...

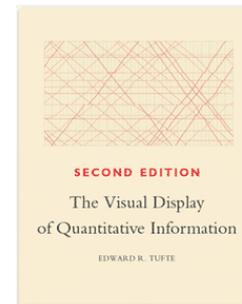
Metrics

Visualization

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

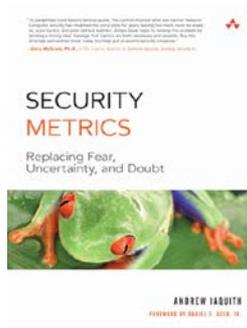


Hubbard, 2014 (3rd ed.)

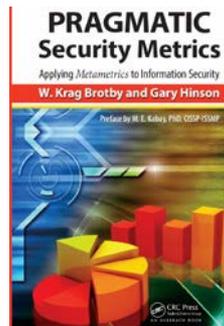


Tufte, 2001 (2nd ed.)

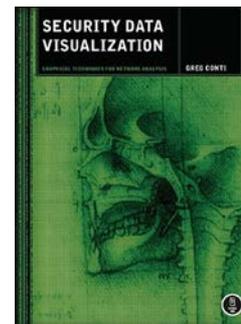
Or, skip to here for content specific to information security (*tactical*)



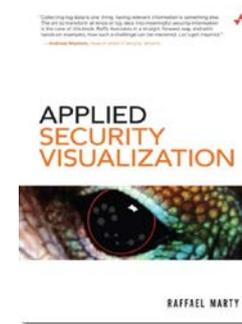
Jaquith, 2007



Brotby & Hinson, 2013



Conti, 2007



Marty, 2008



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

- NIST SP800-55: "Performance Measurement Guide for Information Security"
 - 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



You Want More? Really?

Appendix: Additional Online Resources

• Metrics

- "Security Metrics to Manage Change: Which Matter, Which Can Be Measured?" (Ponemon Institute, 2014) <http://www.ponemon.com/~/media/Files/2014/04/SecurityMetrics.pdf>
- "Security Metrics: Can They Be Effectively Measured Across the Enterprise?" (Alan Shimek et al., 2014) <http://www.rsaonline.com/~/media/Files/2014/04/SecurityMetricsCanTheyBeEffectivelyMeasuredAcrossTheEnterprise.pdf>
- "Technical Metrics Aren't Enough: 10 Strategic Security Measures" (Julia Allen & Lisa Young, 2014) <http://www.rsaonline.com/~/media/Files/2014/04/TechnicalMetricsArenTEnough10StrategicSecurityMeasures2.pdf>
- "No One Cares About Your Security Metrics and You are to Blame" (Paul Proctor, 2013) <http://www.gartner.com/paper/proctor/2013/08/11/no-one-cares-about-your-security-metrics-and-you-are-to-blame/>
- "Measures for Managing Operational Resilience" (Julia Allen & Pamela Curtis, 2011) http://www.rsaonline.com/~/media/Files/2011/05/01_15467.pdf
- "Lord Kelvin Was Wrong" (Ben Tomshaw, 2011) <http://www.rsaonline.com/~/media/Files/2011/03/01/03-01-15476.html>
- "Addressing Mismatch Between Information Security Metrics and Business-Driven Security Objectives" (Christine Fruehwirth, 2010) <http://www.rsaonline.com/~/media/Files/2010/04/01/04-01-15477.pdf>
- "The Center for Internet Security (CIS) Security Metrics v1.0" (CIS, 2010) <http://www.cisecurity.org/cis-security-metrics-v1.0/>
- "Measuring the Success of Your Information Security Programs: Security Metrics" (Rodney Petersen et al., 2009) <http://www.rsaonline.com/~/media/Files/2009/05/01/05-01-15478.pdf>
- "Directions in Security Metrics Research" (Wayne Jansen, 2009) <http://www.rsaonline.com/~/media/Files/2009/05/01/05-01-15479.pdf>
- "Performance Measurement Guide for Information Security" (Elizabeth Chew et al., 2008) <http://www.rsaonline.com/~/media/Files/2008/05/01/05-01-15480.pdf>
- "Measuring Security" (Dan Geer, 2007) <http://www.rsaonline.com/~/media/Files/2007/05/01/05-01-15481.pdf>
- "Choosing the Right Metric" (Zach Geminjan, 2007) <http://www.rsaonline.com/~/media/Files/2007/05/01/05-01-15482.pdf>



© Copyright 2015 EMC Corporation. All rights reserved.

Appendix: Additional Online Resources

• Metrics

- "The Laws of Vulnerabilities: Six Axes for Understanding Risk" (Gerald Eschebeck, 2005) http://www.qualys.com/docs/Laws_Report.pdf
- "Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams" (2004) <https://www.cisecurity.org/~/media/Files/2004/04/04-01-15483.pdf>
- "Patch Management at Microsoft" (Julia Keogh & Paul Thomsen, 2004) <http://www.microsoft.com/research/community/bradford/dotnet/04-01-15484.pdf>
- "Metrics: You Are What You Measure" (John Hauser & Gerald Katz, 1998) <http://web.mit.edu/hauser/www/Papers/hauser-Katz%20Measure%2004-01-15485.pdf>

• Visualization

- "From Data to Wisdom: Big Lessons in Small Data" (Jay Jacobs, 2014) <http://www.rsaonline.com/~/media/Files/2014/04/04-01-15486.pdf>
- "The Heatmap - Why is Security Visualization so Hard?" (Raffael Marty, 2014) <http://www.slideshare.net/rmart/why-is-security-visualization-so-hard>
- "Data Analysis and Visualization for Security Professionals" (Bob Rudis & Jay Jacobs, 2013) <http://www.rsaonline.com/~/media/Files/2013/04/04-01-15487.pdf>
- "Cyber Security - How Visual Analytics Unlocks Insight" (Raffael Marty, 2013) <http://www.slideshare.net/arkano/bdd-2013-dm-challenges>
- "Visualization Design for Immediate High-Level Situational Assessment" (Robert Erbacher, 2012) <http://www.rsaonline.com/~/media/Files/2012/04/04-01-15488.pdf>
- "Security Visualization - Let's Take a Step Back" (Raffael Marty, 2012) <http://www.slideshare.net/rmart/va-sec2012-keynote>
- "Visualizing Host Traffic through Graphs" (Eckard Glatz, 2010) <http://www.rsaonline.com/~/media/Files/2010/04/04-01-15489.pdf>
- "Visualizing Graph Dynamics and Similarity for Enterprise Network Security and Management" (Qiao Liu et al., 2010) <http://www.storm.csi.cmu.edu/papers/2010/04-01-15490.pdf>
- "Introduction to Visualization for Computer Security" (John Goddall, 2007) <http://www.rsaonline.com/~/media/Files/2007/04/04-01-15491.pdf>



© Copyright 2015 EMC Corporation. All rights reserved.

Appendix: Analyst Reports

• Gartner

- "Sharpen Your Security Metrics to Make Them Relevant and Effective" (Rob McMillan, 2014) [G00259303]
- "The Gartner Business Risk Model - A Framework for Integrating Risk and Performance" (Paul Proctor, 2013) [G00247513]
- "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) [G00226999]
- "Why Communication Fails - Five Reasons the Business Doesn't Get Security's Message" (Jeffrey Wheatman, 2011) [G00210798]
- "Five Required Characteristics of Security Metrics" (Jeffrey Wheatman, 2011) [G00212728]
- "Best Practices for Developing a Hierarchy for Security Metrics and Reporting" (Jeffrey Wheatman, 2011) [G00219152]
- "Best Practices for Identity and Access Management Metrics" (Earl Perkins, 2011) [G00210871]
- "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.



© Copyright 2015 EMC Corporation. All rights reserved.

Appendix: Analyst Reports

• Gartner

- "Security and Risk Management as a Social Science" (Tom Scholtz, 2010) [G00206145]
- "The Standard Develops a Practical Model for Implementing Risk Management" (Paul Proctor, 2010) [G00200823]
- "How to Close the Gap Between Information Security and IT Risk Management" (Jeffrey Wheatman, 2009) [G00171441]
- "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 Dots and Dashes of Information Security Metrics" (Jeffrey Wheatman, 2008) [G00162191]
- "A Simple Method for Expressing Information Criticality and Classification" (Jay Heiser, 2008) [G00155346]
- "Toolkit Best Practices: Selecting Security Metrics" (Jeffrey Wheatman, 2007) [G00151310]
- "Relationship Management Is the Least Mature Security Discipline" (Christian Byrnes, 2006) [G00137033]
- "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 Witt, 2004) [TG-22-1617]

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



© Copyright 2015 EMC Corporation. All rights reserved.

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]
- "Determine The Business Value Of An Effective Security Program - Information Security Economics 101" (Ed Ferrara, 2012) [82082]
- "Develop Effective Security Metrics" (Ed Ferrara, 2012) [45787]
- "The Forrester Information Security Metrics 3R Dashboard" (Ed Ferrara, 2012) [87101]
- "The Forrester Information Security Metrics Maturity Model" (Ed Ferrara, 2012) [61232]
- "How to Market Security To Gain Influence And Secure Budget" (Dinan 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.



© Copyright 2015 EMC Corporation. All rights reserved.

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 Kottelz, 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" (Launie Orloy, 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.



© Copyright 2015 EMC Corporation. All rights reserved.



<http://BenSmith.SE/twitter>



<http://BenSmith.SE/linkedin>



Appendix: Additional Online Resources

- Metrics

- "Security Metrics to Manage Change: Which Matter, Which Can Be Measured?" (Ponemon Institute, 2014) <http://content.firemon.com/PonemonSecurityMetricsAndChangeSurveyResults>
- "Security Metrics: Can They Be Effectively Measured Across The Enterprise?" (Alan Shimel *et al.*, 2014) http://www.rsaconference.com/writable/presentations/file_upload/ciso-w01-security-metrics-can-they-be-effectively-measured-across-the-enterprise_copy3.pdf
- "Technical Metrics Aren't Enough: 10 Strategic Security Measures" (Julia Allen & Lisa Young, 2014) http://www.rsaconference.com/writable/presentations/file_upload/grc-f01-technical-metrics-arent-enough-10-strategic-security-measures_2.pdf
- "No One Cares About Your Security Metrics and You are to Blame" (Paul Proctor, 2013) <http://blogs.gartner.com/paul-proctor/2013/08/11/no-one-cares-about-your-security-metrics-and-you-are-to-blame/>
- "Measures for Managing Operational Resilience" (Julia Allen & Pamela Curtis, 2011) http://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15407.pdf
- "Lord Kelvin Was Wrong" (Ben Tomhave, 2011) <http://www.secureconsulting.net/2011/03/lord-kelvin-was-wrong.html>
- "Addressing Misalignment Between Information Security Metrics and Business-Driven Security Objectives" (Christian Fruehwirth, 2010) <https://www.sba-research.org/wp-content/uploads/publications/a6-fruehwirth.pdf>
- "The Center for Internet Security (CIS) Security Metrics v1.1.0" (CIS, 2010) https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf
- "Measuring the Success of Your Information Security Programs: Security Metrics" (Rodney Petersen *et al.*, 2009) <http://www.nchica.org/Past/AMC09/presentations/Security/Petersen.pdf>
- "Directions in Security Metrics Research" (Wayne Jansen, 2009) http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf
- "Performance Measurement Guide for Information Security" (Elizabeth Chew *et al.*, 2008) <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>
- "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

- "The Laws of Vulnerabilities: Six Axioms for Understanding Risk" (Gerald Eschelbeck, 2005) <http://www.qualys.com/docs/Laws-Report.pdf>
- "Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams" (2004) <https://net.educause.edu/ir/library/pdf/CSD3661.pdf>
- "Patch Management at Microsoft" (Brian Keogh & Paul Thomsen, 2004) <http://www.microsoft.com/technet/community/tnradio/rdotrns01.msp>
- "Metrics: You Are What You Measure!" (John Hauser & Gerald Katz, 1998) <http://web.mit.edu/hauser/www/Papers/Hauser-Katz%20Measure%2004-98.pdf>

- Visualization

- "From Data to Wisdom: Big Lessons in Small Data" (Jay Jacobs, 2014) http://www.rsaconference.com/writable/presentations/file_upload/cds-t07-from-data-to-wisdom-big-lessons-in-small-data.pdf
- "The Heatmap - Why is Security Visualization so Hard?" (Raffael Marty, 2014) <http://www.slideshare.net/zrlram/the-heatmap-why-is-security-visualization-so-hard#>
- "Data Analysis and Visualization for Security Professionals" (Bob Rudis & Jay Jacobs, 2013) http://www.rsaconference.com/writable/presentations/file_upload/grc-t18.pdf
- "Cyber Security - How Visual Analytics Unlock Insight" (Raffael Marty, 2013) <http://www.slideshare.net/zrlram/kdd-2013-dm-challenges>
- "Visualization Design for Immediate High-Level Situational Assessment" (Robert Erbacher, 2012) <http://users.soe.ucsc.edu/~pang/visweek/2012/vizsec/17-Erbacher.pdf>
- "Security Visualization - Let's Take a Step Back" (Raffael Marty, 2012) <http://www.slideshare.net/zrlram/viz-sec2012-keynote>
- "Visualizing Host Traffic through Graphs" (Eduard Glatz, 2010) <http://www.vizsec.org/files/2010/Glatz.pdf>
- "Visualizing Graph Dynamics and Similarity for Enterprise Network Security and Management Security and Management" (Qi Liao *et al.*, 2010) <http://www.vizsec.org/files/2010/Liao.pdf>
- "Introduction to Visualization for Computer Security" (John Goodall, 2007) <http://web.ornl.gov/~ojg/goodall-vizsec07.pdf>

Appendix: Analyst Reports

- Gartner

- "Sharpen Your Security Metrics to Make Them Relevant and Effective" (Rob McMillan, 2014) [G00259303]
- "The Gartner Business Risk Model - A Framework for Integrating Risk and Performance" (Paul Proctor, 2013) [G00247513]
- "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]
- "Why Communication Fails - Five Reasons the Business Doesn't Get Security's Message" (Jeffrey Wheatman, 2011) [G00210798]
- "Five Required Characteristics of Security Metrics" (Jeffrey Wheatman, 2011) [G00212728]
- "Best Practices for Developing a Hierarchy for Security Metrics and Reporting" (Jeffrey Wheatman, 2011) [G00219152]
- "Best Practices for Identity and Access Management Metrics" (Earl Perkins, 2011) [G00210871]
- "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]
- “The Standard Develops a Practical Model for Implementing Risk Management” (Paul Proctor, 2010) [G00200823]
- “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]
- “Toolkit Best Practices: Selecting Security Metrics” (Jeffrey Wheatman, 2007) [G00151310]
- “Relationship Management Is the Least Mature Security Discipline” (Christian Byrnes, 2006) [G00137033]
- “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]
- "Determine The Business Value Of An Effective Security Program — Information Security Economics 101" (Ed Ferrara, 2012) [82082]
- "Develop Effective Security Metrics" (Ed Ferrara, 2012) [45787]
- "The Forrester Information Security Metrics 3R Dashboard" (Ed Ferrara, 2012) [87101]
- "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.

