Lattice

Information Security and Compliance Metrics

Pragmatic measurement

Walter Williams

January 25, 2013

Metrics

- What are metrics as understood by ISO 2700x
  - Not just something that can be measured
  - The result of the analysis of multiple measure sources through an algorithm which allows you to express the delta between the desired performance and the existing performance
    - You must identify
      - Base measures
      - Measurement methods, scale, unit of measure
      - Analytical Model
      - Decision Criteria
    - You must measure the maturity of your metrics

Goal Oriented Metrics

- What has the business defined as its goals?
- How does the ISMS fit into that?
- How do you measure when you're being successful
  - Your metric is the gap between the goal and the reality

Difference between metrics and measurements

- A measurement tells you how much or how often
  - Your anti-virus blocked 30,000+ incidents last quarter
  - Your anti-virus failed to block 10 incidents last quarter
- Those are measurements
  - What do they tell you?
  - Is your anti-virus effective?
  - Can you tell from those numbers?
    - No.
- Metrics are the analysis of measurements designed to answer questions such as “is it effective”

Lattice

Metric Maturity

- Pragmatic Metrics
  - A model for measuring the maturity of your metrics
    - Predictive
    - Relevant
    - Actionable
    - Genuine
    - Meaningful
    - Accurate
    - Timely
    - Independent
    - Cost effective to measure

Predictive measurements

- Information Security and Compliance Metrics are often expressed by what didn't happen or hasn't happened yet
  - Breaches: 0
    - Numbers like these are often good indicators of success, but are not predictive
  - Change in the number of accepted Risks with an impact of over 1M over the last 12 months: Down by three from 12
    - Numbers like this are still not very predictive
    - Sound risk management does not always decrease # of accepted risks

Predictive measurements

- Person hours to respond to Customer's remediation demands

	Customer1	Customer 2	Customer 3
Time needed to respond to Security Survey (in hours)	40	40	80
Tickets created to prepare for an audit	0	31	8
Time needed to prepare for an audit (in hours)	0	155	40
Tickets created in response to an audit	0		35
Time needed to respond to an audit (In hours)	0		175
Onboarding Tasks	5		2
Onboarding Hours (Estimated)	1920		

- There may be a trend here. As we track more on this, these measures can help us develop predictive metrics.

Relevant Metrics

- 99.999 Uptime is a great metric
  - Shows operational success
  - Tells you nothing about the information security goal of availability
- DDoS attacks in each of the last 4 Quarters
  - This is not predictive
  - But does inform regarding the IS goal of availability

Actionable

- 114 Laptops encrypted is a great measurement of success
  - But what do you do with it?
- 95% of critical vulnerabilities detected on servers are found in Non-OS components over the last six month are unpatched Java and Adobe
  - This is actionable

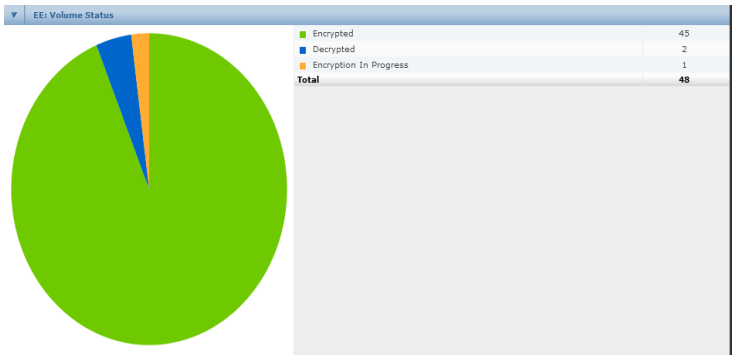
Genuine

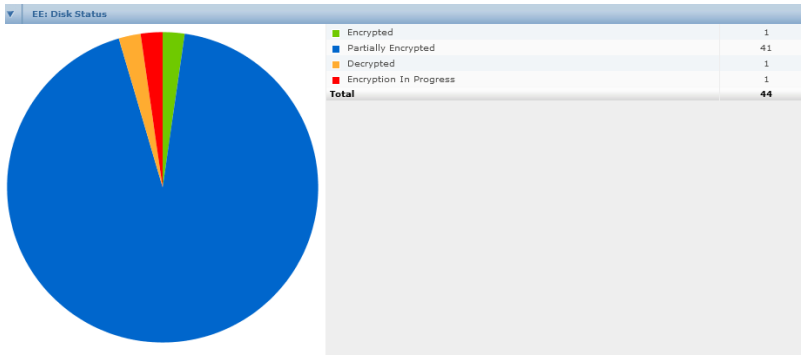
- 0 Breaches in the last year!
  - Oh? And how do we know this?
  - Perhaps 0 detected breaches
  - Our metrics must always be genuine

Meaningful

- 54 Emails Identified as SPAM per day!
  - How many were not identified but were spam?
  - We don’t want metrics that just show churn
  - Number of tickets opened to complain about SPAM per month
    - That is meaningful, and tracked over time can be predictive

Accurate





We will need to verify what our tools tell us

Timely

- Number of Vulnerabilities in a branch office in June of 2012: 647
  - Who cares, most of those servers don't even exist any more
- Number of Vulnerabilities on New Production Servers as of March 31, 2016
  - 117 on 9 hosts

Independent

- As in independent of the observer
  - The metric must be objective

Cost effective to measure

- Cost effective is not just how expensive it is to measure
- Which depends often on how frequently you perform the measurement
- And how long it takes to take the measurement
  - # of unresolved tickets: 43
- It is also how much value do you get from the measurement
  - Ratio of unresolved Security tickets with open for more than 30 days to Rest of Tickets open for more than 30 days to % of Budget dedicated to Security

What to measure?

- Security
- Compliance

Compliance Metrics

- Compliance
  - With Policy
  - With Standards
  - With Procedures
  - With Laws

  - **If** our Policies, Procedures and Standards manage risk effectively
  - **And if** we are COMPLIANT with them, we are relatively secure
  - We can measure to what degree we are compliant with our policies, procedures and standards.

  - There are some dangerous assumptions here

Lattice

Deriving metrics

- Some times the raw measurements inform on the success of your goals:
  - Goal – 0 incidents with data breaches
  - Measurement & metric are the same here

- ISO 27004 recommends:
  - Easily repeatable process
  - Easily derived measurements from data at hand
  - Informs on the effectiveness of your system

Lattice

Metrics at Lattice

- Used our policy as the framework
  - Established a goal for each section
    - Goal oriented metrics derive value from consistently measuring the delta from the stated goal
  - Identify measurements that inform success regarding that goal
  - Identify the relationship between those measurements
    - Some times that is a proportion, some times it is more complex
  - The metric is the goal
  - Report on the delta

Lattice

What did the introduction of metrics reporting do?

- Vulnerabilities plunged 98%
  - Only vulnerabilities in production are new per month
- Unauthorized changes plunged 100%
  - No one wants to get caught twice
- Confidence in our DR strategy rose
  - When you do a recovery a month successfully, people stop worrying
- 10% of metrics were adjusted over the last six months
- Pain points became identified
  - Automation can’t solve all problems

Lattice

Some notes on Lattice's IS metrics

- All metrics meet the criteria for measuring the effectiveness of IS as per ISO 27004
- We don't have a dashboard or a fancy way to report
  - Yet
  - We let the numbers do the talking, but we're a data analytics company
    - We like numbers
- Planned improvements
  - Use of the Thomas Scoring System?
    - http://exploringpossibilityspace.blogspot.com/2014/02/thomas-scoring-system.html
  - This is complex, but provides hope of properly aggregating unrelated information
  - Dashboard?
- Goals are realistic, not idealistic
  - Risk never is 0

Lattice

Lattice

Now for the sample metrics

Risk Management

- Impact Value of Unremediated risks/ Impact Value of Total Risks
  - Don’t do math, show the raw numbers as a comparison rather than a division
  - Amount of total risk is expected to grow as the company becomes more successful, the impact of the unremediated risk should not grow with the value of the firm, having proportionally less of a potential impact
- Goal: Impact Value of Unremediated risks/ Impact Value of Total Risks shrinks over time
- This will show the reduction in impact through the application of remediation. In essence this should, over time, equal the risk value of accepted risks.
- Report to: Executive Team
- Frequency: Quarterly

Lattice

Effectiveness of Security Policy

- # of internal security issues
- Security issues come from individuals seeking to bypass controls to perform job functions effectively. Most incidents shows an ineffective control which needs to be adjusted or tuned.
  - There is an exception here: a repeat offender
- Goal:0 Internal Security Issues
- Report to: Executive Team
- Frequency: Quarterly

Lattice

Value of ISMS to Lattice

- $ of bookings with security surveys/Total $ of bookings
- This shows the impact to the business of running an effective security program as the percentage derived would be an inverse value if the ISMS was not effective in the eyes of its customers
- Goal: Value is positive
- Report to: Executive Team
- Frequency: Quarterly

Lattice

Asset management gap

- (# hosts identified in vuln. scans - # hosts in inventory) + # of hosts in inventory without owner.
- This number, which should be 0, identifies a failure to maintain the asset inventory
- Goal: 0
- Report to: Director of Technology Services
- Frequency: Quarterly

Lattice

Security Awareness Level

- # of questions answered wrong * number of respondants / # of questions * number of employees
- This ratio, which should be 0, shows the retention of security awareness information throughout the enterprise.
- Goal: 0
- Report to: Director of HR
- Frequency: Annually

Lattice

Security of Operations

- # of change records created / # of changes to platform standards
- Instead: # of change records created with sufficient data for some one else to perform change or back out change/ Total # of changes
- Lack of well formed descriptions of changes, test plans and back out plans impact value of CR process
- Goal: 1
- Report to: Director of Technology Services
- Frequency: Quarterly

Lattice

Completeness of Recoverability

- Systems + databases / backup jobs
- Instead databases/backup jobs
- This metric should be 1 or more
- Goal: 1
- Report to: Director of Technology Services
- Frequency: Quarterly

Lattice

Completeness of monitoring

- # of systems monitored/# of systems
- Could also look at # systems * # Protocols monitored/# total systems * # Protocols
- This metric should show a value of 1, indicating we are monitoring 100% of all systems
- Goal: 1
- Report to: Director of Technology Services
- Frequency: Quarterly

Lattice

Non-Conformance to Access Control Policies

- # of accounts not in conformance with LE policies/# of accounts)* user accounts assigned permissions without group membership
- This ratio, which should be 0, shows the percent deviation from the policy.
- Goal: 0
- Report to: Manager of IT
- Frequency: Quarterly

Lattice

Security of Engineering

- CVSS of Vulnerabilities Remediated in Bugs * number of vulnerabilities remediated/CVSS of Vulnerabilities not remediated in released code * number of unremediated vulnerabilities
- Instead 8 * (number of CVSS 7-10 rated issues) patched + 2 * (number of CVSS 4-6 rated issues) patched compared to 8 * (number of CVSS 7-10 rated issues) unpatched + 2 * (number of CVSS 4-6 rated issues) unpatched
  - (unpatched / patched)
- This shows the residual risk of unpatched issues per release
- Goal: 0
- Report to: VP of Engineering, Director of Engineering and Director of QA
- Frequency: Quarterly

Lattice

Unpatched critical vulnerabilities per data center

- # of critical vuln still present post patch
  - Critical Vulnerabilities are defined as those for which an exploit is avialable
- This will show the effectiveness of the vulnerability management procedure. The results should be 0.
- Goal: 0
- Report to: Director of Technology Services
- Frequency: Quarterly

Lattice

Penetration Tests

- Here you don't want to look at a vulnerability unless it is an exploitable vulnerability. The goal isn't a perfect system, the goal is a secure system.
- By exploitable, we're concerned against compromise of:
  - Confidentiality, Availability, Integrity, Control, Utility, Authenticity, & Privacy
- Goal: 0 paths to compromise the integrity, confidentiality, availability, control, authenticity, utility or privacy of our customer's data
- Report to VP of Engineering
- Frequency: Per release cycle

Lattice

Realized security incidents

- Number of security incidents requiring remediation/number of security incidents
- This measures the number of security incidents that were real, rather than false positives. By measuring the difference, it shows that the incident management program tests for false positives and works to remediation all actual incidents. Results should be either 0, or 0/0, which will be considered 0 for this metric
- Goal: 0
- Report to: Executive Team
- Frequency: Quarterly

Lattice

Business Continuity

- Number of services available to company during continuity test/number of services available normally
- Instead, number of tickets raised during BC testing related to inability to perform job. Number should be 0
- If this relationship is not 1, then there were services which were not properly planned for in the BCP plan, which will need to be adjusted to address the root cause of this failure of availability
- Goal: 0 tickets
- Report to: Executive Team
- Frequency: Annually

Lattice

Number of third party audit findings

- # of Findings / Number of Controls selected for implementation.
- If this value is 0, then the ISMS is achieving 100% of the goals identified in the standards.
- Report to: Executive Team
- Frequency: Annually

Lattice

Questions?

- Staying in touch:
- wwilliams@lattice-engines.com
- Walt.williams@gmail.com

- @LESecurity

- http://infosecuritymetrics.wordpress.com/

Lattice