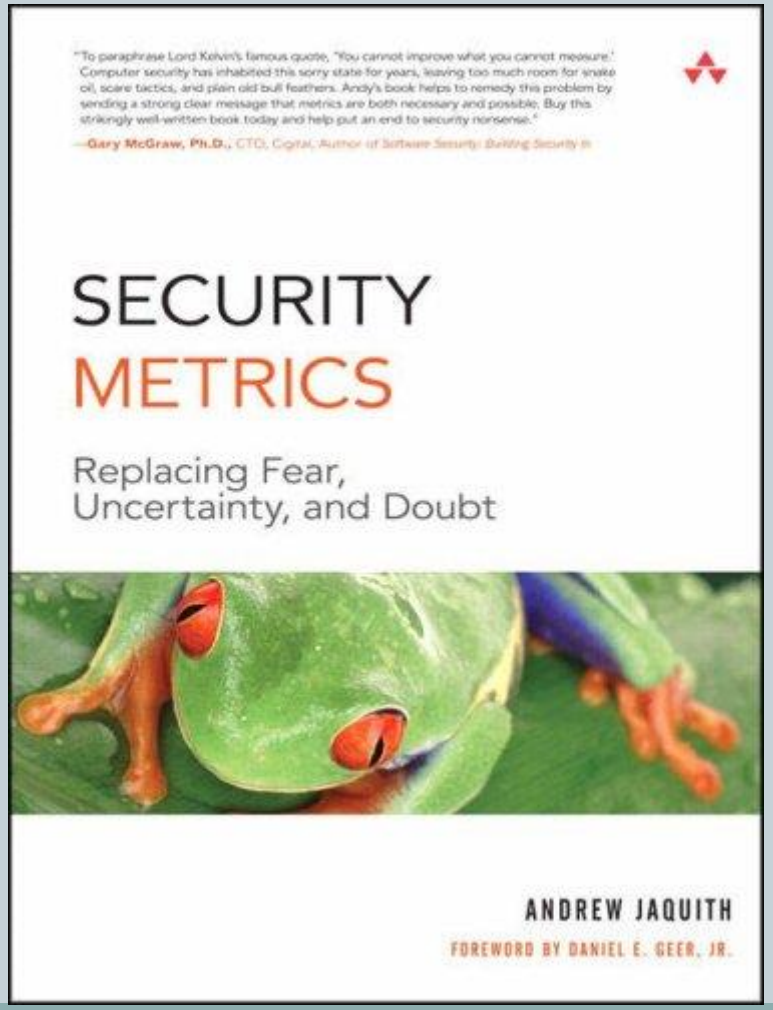
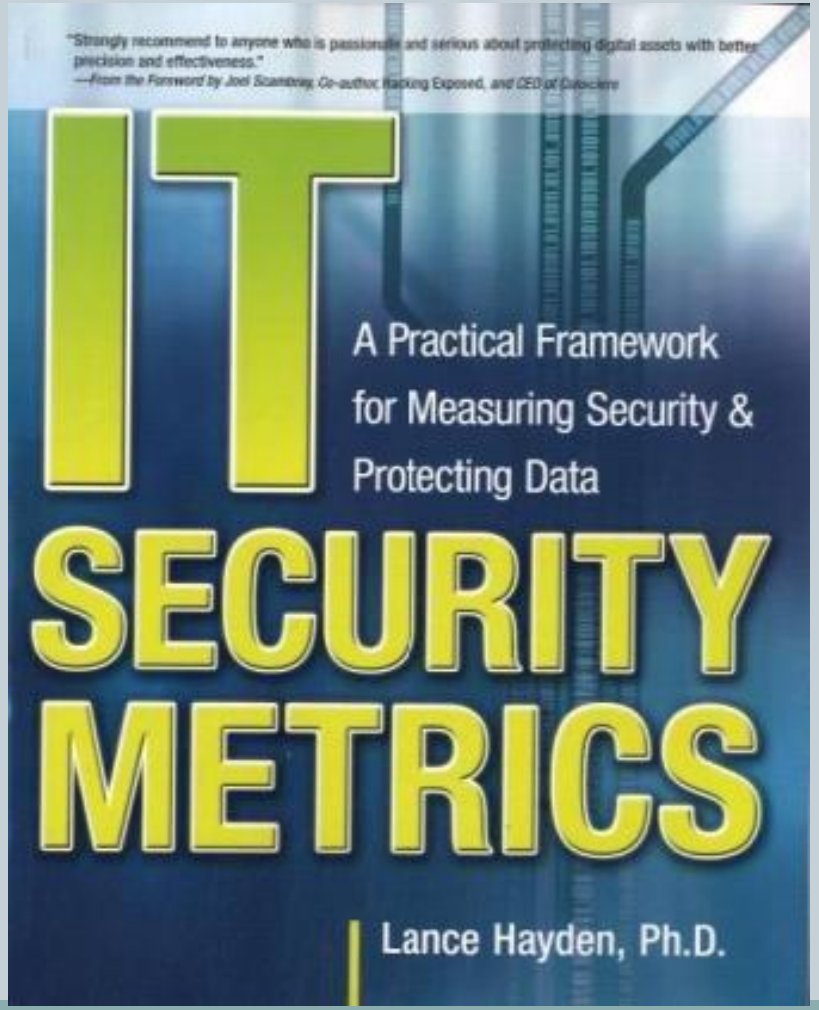
Security Metrics

WHO? WHY? WHAT ? HOW?

What are Security Metrics ?

Want to know more…





Measurements vs. Metrics – same thing?

Measurements	Metrics
• Single-point-in-time views of specific, discrete factors • Generated by counting • Objective raw data	• Derived by **comparing** two+ measurements taken over time to a predetermined baseline • Generated by analysis • Objective or subjective interpretations of those data

The Mark of Good Metrics

Metrics should be SMART	
Specific	Well-defined, using unambiguous wording
Measurable	Quantitative when feasible
Attainable	Within budgetary and technical limitations
Repeatable	Measurements from which metric is derived do not vary depending on the person taking them.
Time-dependent	Takes into consideration measurements from multiple time slices

George Jelen, "SSE-CMM Security Metrics"

Rate These Metrics

- % of servers that are secure
- % of employees who are aware of security threats
- # of unauthorized accesses to sensitive data
- % of total IT budget spent on security
- Web application vulnerabilities found during July 2008 penetration test

What about this ?

- AV – How many viruses are being caught
- How many systems have AV and
- How many of those have up to date definition files
- Patch latency – time period that system is patching isn't up to date increases the risk to that system and org.
- Are these good ?

Truly Useful Metrics…

- Indicate the degree to which security goals are being met
- Show and enable a (strong) linkage between security and organisational goals
- Inform actions which can be taken to improve the overall security program
- Allow for the monitoring of perfomance over time

Good Metrics

- Baseline Defenses Coverage (AV, FW, etc)
  - Measurement of how well you are protecting your enterprise against the most basic information security threats.
  - 94% to 98%; less than 90% cause for concern
- Patch Latency
  - Time between a patch's release and your successful deployment of that patch.
  - Express as averages and criticality
- Platform Security Scores
  - Measures your hardening guidelines
- Compliance
  - Measure schools/departments against security standards

The Value of Security Metrics

- Discern the effectiveness of a particular component of a security program
- Indicate the security of a specific system, product, or process
- Identify the risk in **not** taking a given action and, thereby, help prioritize corrective actions
- Provide evidence of regulatory compliance
- Raise the level of security awareness among executives and other stakeholders
- Show contribution of security to meeting institutional goals and objectives

The Value of Security Metrics II

- Demonstrate the ability of security teams & (client) departments to address security issues for which they are responsible
  - Influence is often data dependent
  - Measurement is needed
  - ROI ?
- Provide basis for security managers to answer tough questions, such as
  - *Are we more secure today than we were before?*
  - *How do we compare to others in this regard?*
  - *Are we secure enough?*
- Prove you are doing your job
  - *Nobody notices when nothing breaks.*

What metrics cant do

- We can’t answer
  - “How secure am I?”
  - “Where should I place my security resources?”
  - “Am I spending Enough (or too much) ?”
- Cannot replace existing security practice
- Cannot allow omniscient Intel
- Cannot be the only decision making tool

State of Security Metrics Today
(or, why developing good metrics can be challenging)

How useful is this metric?

Reported data breaches increased sharply in the first six months of 2008, jumping 69 percent compared to the same period last year, according to a study by the Identity Theft Resource Center (ITRC). But the percentage of breaches occurring in the government sector has dropped steadily in the past three years.

July 2, 2008

Consider the statement with this in mind

- Unlike private industry, governmental and educational institutions have historically (?) been quite open about incidents that occurred.
- Increasingly, state laws are requiring both private and public sector entities to report incidents.
- Organizations with poor security programs don't know when breaches occur.
- Impact of Incident A ≠ Impact of Incident B

Bottom-line: The metric reveals nothing about institutional risk

How To Measure Risk?

Risk = Asset Value x Threat x Vulnerability

- **Asset Value** – easiest to measure in some cases, but how to quantify assets like institutional reputation?
- **Threat** – very hard to measure the potential for harm, although information from external sources may be useful.
- **Vulnerability** – CIS benchmarks and output from other tools provide good information, but not all vulnerabilities can be quantified.

The State of Security Metrics Research

- In the last few decades, Information Security has gained numerous standards, industrial certifications, and risk analysis methodologies.
- However, the field still lacks the strong, quantitative, measurement-based assurance that we find in other fields.
- Security looks different. Even a fairly sophisticated standard such as ISO17799 has an intrinsically qualitative nature.
- Furthermore, many recorded security incidents have a non-IT cause.
- As a result, security requires a much wider notion of "system" than do most other fields in computer science. In addition to the IT infrastructure, the "system" in security includes users, work processes, and organizational structures.
- Growth of Conferences
- Websites – securitymetrics.org

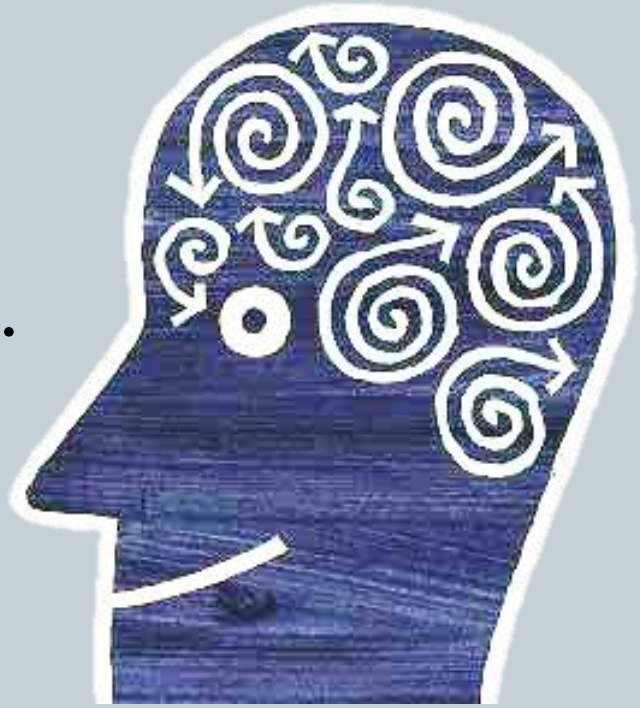
Building Metrics

Be SMART

- But not too smart…

Be SMARTer

- What are you trying to achieve?
- What are you trying to measure ?
- Can you get the data ?
- Will this really be of value ?
- Resist the urge for pretty pictures.



One approach

- The 7-step programme
  - Iterative process
  - Taken from work done by **SHIRLEY C. PAYNE**

Seven-Step Methodology

Step 1

Define the metrics program goal(s) and objectives

- Clearly state the end toward which all metrics and measurements should be directed
- Indicate high level actions that must be collectively accomplished to meet the goal(s)

Step 2

Decide what metrics to generate

- Use existing process improvement framework to determine metrics

  EXAMPLE: *In compliance-based framework, a metric might be the degree of increase in ISO 17799 compliance since standard adopted, based on audit findings.*

- In the absence of or in addition to pre-existing framework, use top-down or bottom-up approach for determining what metrics might be desirable

Top-down Approach

STEPS	EXAMPLES
a. Define/list objectives of the overall security program	*To reduce the number of virus infections within the institution by 30% by 2010*
b. Identify metrics that would indicate progress toward each objective	*Current ratio of viruses in the wild to actual infections as compared to the baseline 2008 figure*
c. Determine measurements needed for each metric	*Number of virus in the wild as reported by abc external source* *Number of virus infections detected*

Bottom-up Approach

STEPS	EXAMPLES
a. Identify measurements that are/could be collected for this process	*Monthly number of critical vulnerabilities detected in servers using xyz scanning tool*
b. Determine metrics that could be generated from the measurements	*Change in number of critical vulnerabilities detected in servers since xyz scanning tool implemented*
c. Determine the association between the derived metrics and established objectives of the overall security program	*To reduce the number of detectable vulnerabilities on servers by 95% by 2009.*

Step 3

Develop strategies for generating the metrics

- Identify sources of data
  - IT groups (help desk, network engineers, application developers, ….)
  - Auditors
  - Training
  - Emergency management
- Decide on frequency of data collection
- Assign responsibility for assuring accuracy of raw data
- Develop methods for compiling data into measurements and generating metrics

Step 4

Establish benchmarks and targets

- Research observed trends and recommendations from professional associations, published research, etc.
- Set reachable targets

Step 5

Determine how the metrics will be reported

- Effective communication of metrics is obviously key. Don't over-simplify, but present clearly.
- Vary what is reported and how depending upon audience:
  - Security manager and staff
  - Department managers
  - Executives
- Determine context, format, frequency, distribution method, and reporting responsibility

Step 6

Create an action plan and act on it

- Plan and conduct actions needed to generate metrics; test and verify; implement

Step 7

Establish a formal program review and refinement cycle

- Is there doubt about the accuracy of some of the metrics?
- How much effort is required to generate the metrics? Are they worth it?
- Are there new security metric standards and effective practices to consider?
- And most importantly, have the metrics guided improvement to the overall security program?

Step 7a

Actually implement and update

- Rinse and Repeat
- This may well be the hardest part
- Remember SMART ?
- A metrics system should not be totally rigid, and should evolve
- Integration with change controls, and other ‘hooks’ into operational activities

Where to Start

- Figure out who the metrics will be reported to
  - Security Officer
  - CIO
  - Chancellor/President
  - Oversight Board
- Understand what is relevant to your audience
  - Technical Vs. Management
    - Technical: 100 viruses blocked, 2 missed = 98% success rate
    - Management: Business impact: 2 missed viruses led to 20 man-hours to control, and may have exposed sensitive data.

Where to Start cont'd

- Metrics Basics
  - Know what is important
  - Risk analysis is a must
  - Identify incident trends that matter to key senior managers
  - Develop a few value indicators that provide reliable information that you can track
  - Set up a security council
  - Track changes
  - Use metrics in planning
  - Check your numbers

Who Needs What?

- Security Officer
  - Operational Metrics
    - Helps to “see” the big picture
  - Compliance Metrics
    - Measured against your regulations/requirements/standards
    - Where the issues are at
  - Project Metrics
    - Show Return On Security Investment (ROSI)
    - Derived from Operational Metrics
  - Need metrics to inform and advise senior management in managing risk. Manage and improve security processes.

Who Needs What? II

- CIO
  - Project Metrics
  - Compliance Metrics
  - Maybe Operational Metrics
    - Especially as they may relate to the other IT functions
  - Risk
    - May not want to know specific metrics just what the risks are
    - Security Posture
  - Time Metrics
    - Operational efficiency, reduced cycle time
  - Financial Metrics
    - Increased productivity, lower costs, lower headcount
  - Ask what they want and what concerns them
    - Translate into how the security program can support it and other priorities or the organization

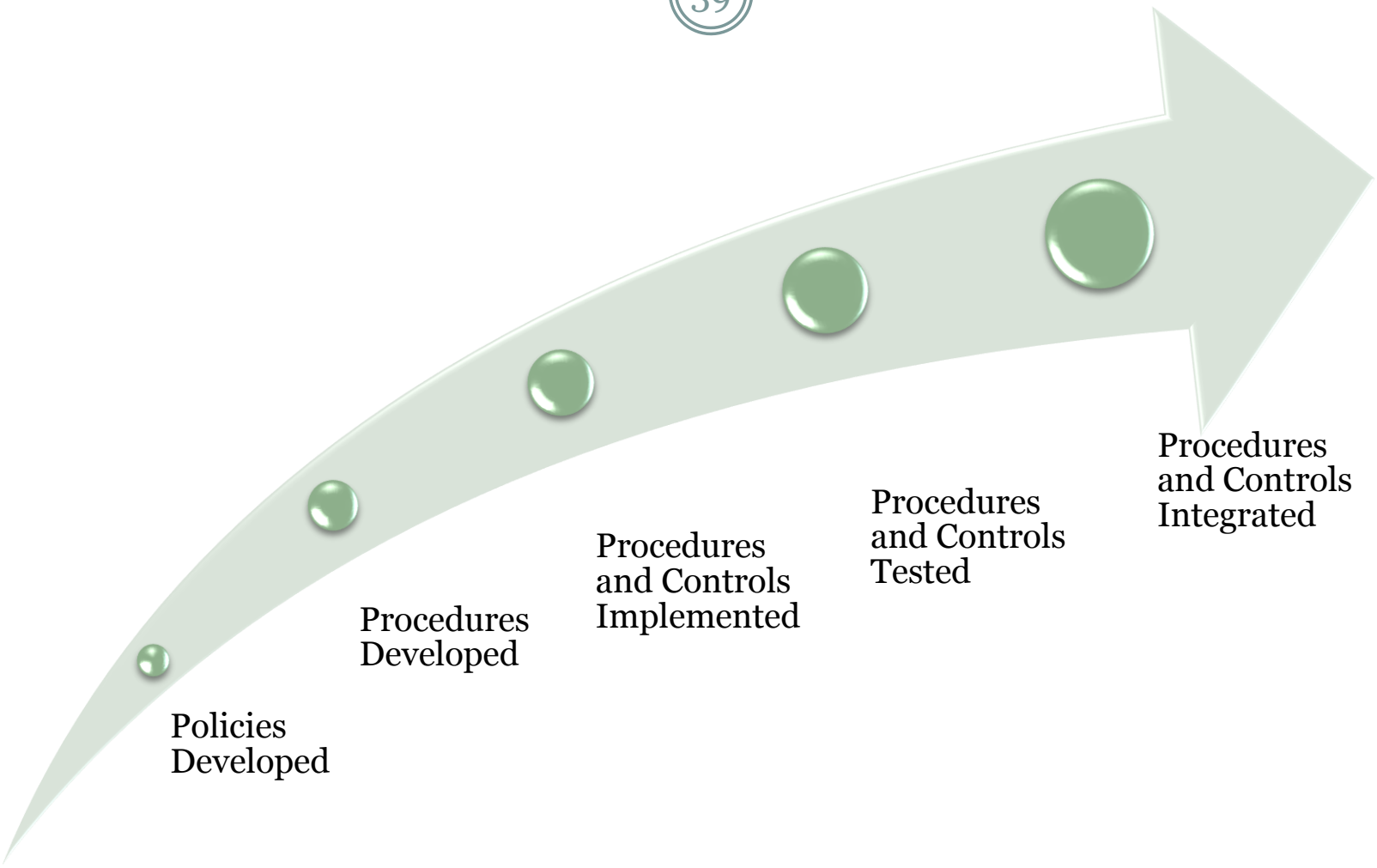
Who Needs What? III

- Chancellor/President/Board
  - Risk
    - What is the overall security posture of the organization
    - What risks exist that would impact our brand
  - Compliance Metrics
    - Confidence in external reporting of regulatory compliance, enterprise risk management status, how do we compare to peers?
  - Ask what they want and what concerns them
    - Translate into how the security program can support it and other priorities of the organization

Planning for success

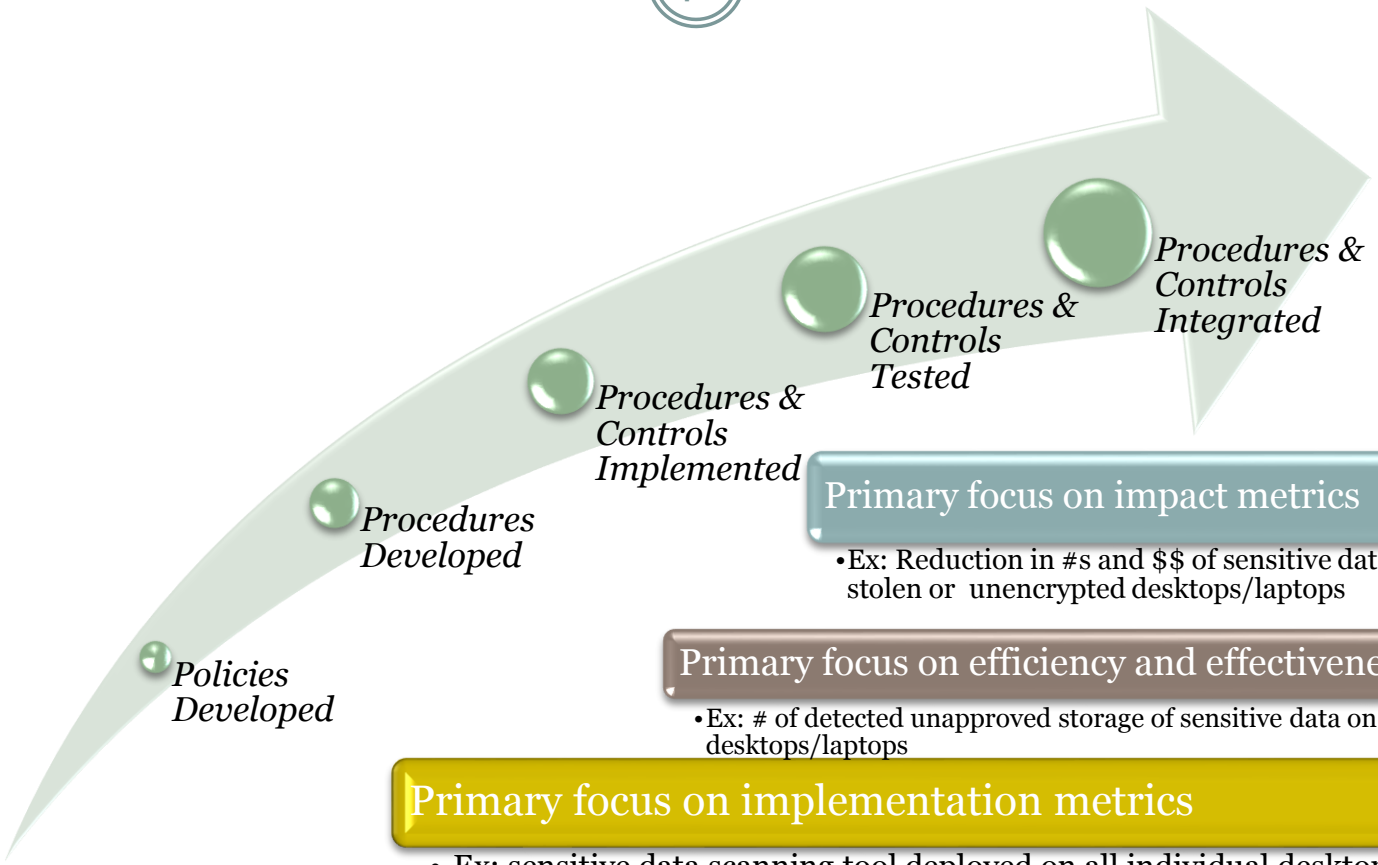
- Gain executive level support
- Use only practical metrics, i.e. those that rely on data that can be **cost-effectively obtained** and assumed to be accurate. Timeliness is also important.
- Focus on quantifiable metrics
- Tailor presentation of metrics to the audience
- Ditch metrics that do not:
  - demonstrate the degree to which goals and objectives of the overall security program are being met; or
  - identity new needs
- Keep the metrics program manageable – track just a few per audience. The temptation is to overwhelm.
- Ensure that the metrics tracked stay meaningful

Usefulness of a Given Metric Varies Depending Upon Maturity of the Security Program



NIST SP 800-26

Usefulness of a Given Metric Varies Depending Upon Maturity of the Security Program



Primary focus on impact metrics

- Ex: Reduction in #s and $$ of sensitive data exposures due to stolen or unencrypted desktops/laptops

Primary focus on efficiency and effectiveness metrics

- Ex: # of detected unapproved storage of sensitive data on desktops/laptops

Primary focus on implementation metrics

- Ex: sensitive data scanning tool deployed on all individual desktops/laptops

Useful metrics difficult to produce at this early stage; limited availability of data and collection may be difficult

NIST SP 800-26

Metrics, Pictures and Dashboards

MAKING THE DATA PRETTY SO EVERYONE BELIEVES YOU….

On stats….

Figures often beguile me, particularly when I have the arranging of them myself; in which case the remark attributed to Disraeli would often apply with justice and force:

"*There are three kinds of lies: lies, damned lies and statistics.*"

- Mark Twain's Own Autobiography: The Chapters from the North American Review

Dogbert's Take on Metrics

Cave..


THINGS TO BEWARE OF:
dogs
strangers
STATISTICS
LUNCHBREATH

Tools and Reporting

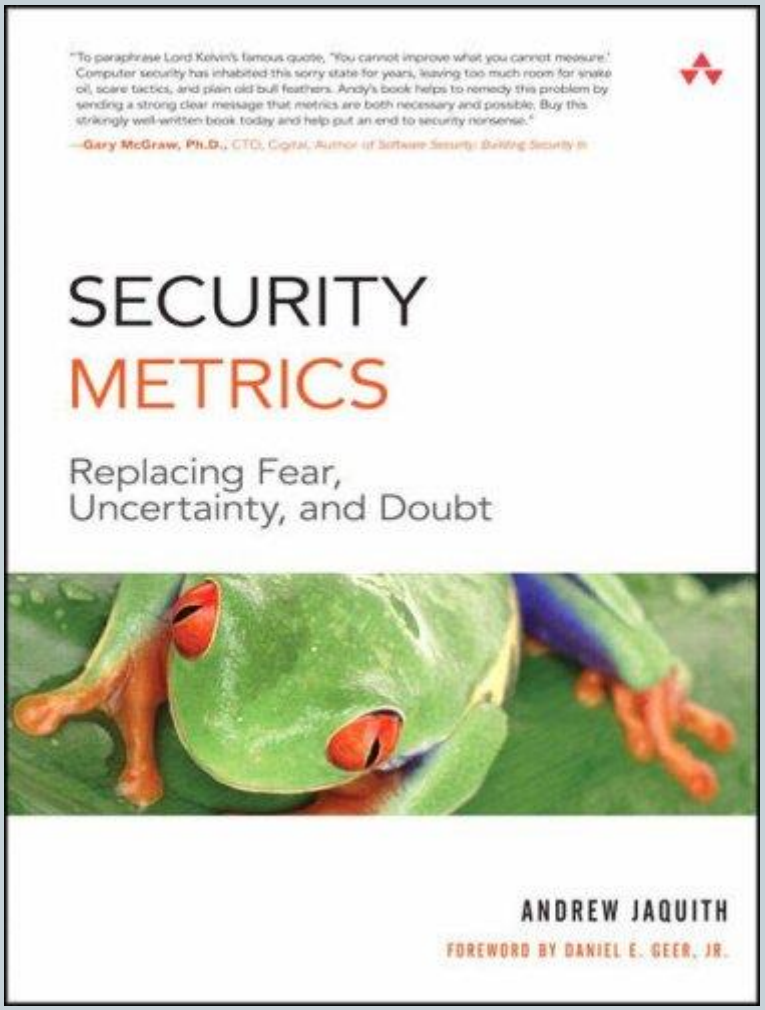
- Automated tools
  - ClearPoint Metrics for dashboard
  - Network scanning tools
  - AV console
  - Excel
  - Custom tools
- Dashboards
  - Graphs
  - Charts
  - Visualize the data (especially for executives)

Good Metric Viz

- Don’t oversimplify
- Don’t be overly ornate
- Do use a consistent scale
- Do include a benchmark

- *Lots of research being done on Security Visualisation (secviz)*

Visualisation



- Chapter 6
- If you only read one chapter let this be it.
- Freely available online as a sample chapter
- http://media.techtarget.com/searchSecurity/downloads/Security_Metrics_-_Ch._6.pdf

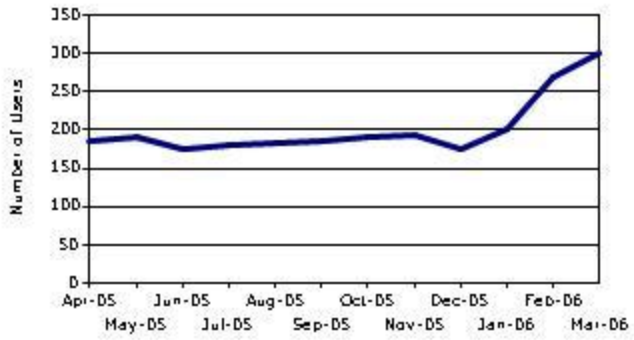
Identity and Access Management Scorecard

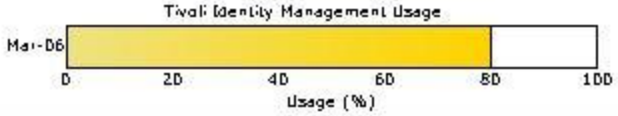
ClearPoint METRICS

Objective

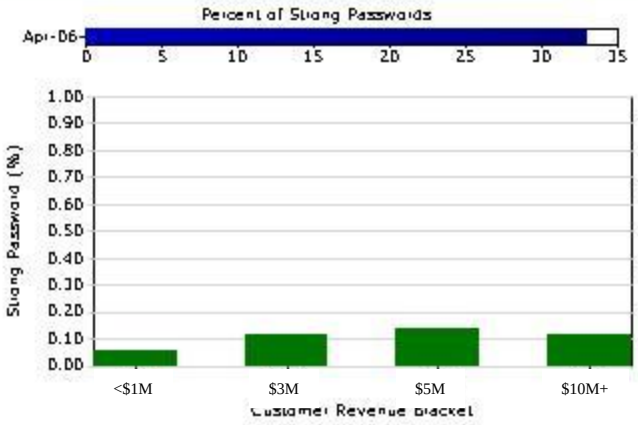
This scorecard is designed for the business manager of the web portal. The scorecard is divided into four quadrants, focusing on usage, access controls, support response, and costs. The upper left quadrant tracks login activity in terms of number of monthly logins. Specific metrics that were requested include FIM usage as a percent of monthly logins and the current percentage of TIM fields that are populated. The upper right quadrant provides metrics on the security state of the portal login accounts, showing the current overall percentage of strong passwords. Time to deprovision accounts are shown as an indicator of the quality of the access control processes. The lower left quadrant shows the overall level of support activity, with key support activities separated from general activities. Along with quantity, the average response time is trended, for key support activities as well as general activities. The final quadrant ties the portal activity to costs.

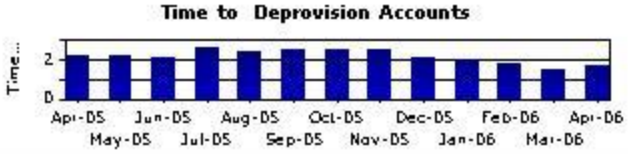
Usage





Access Control Performance

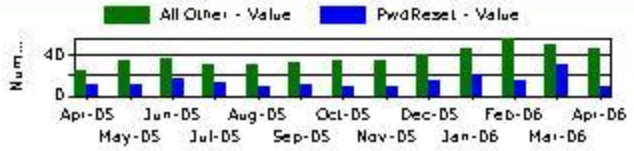


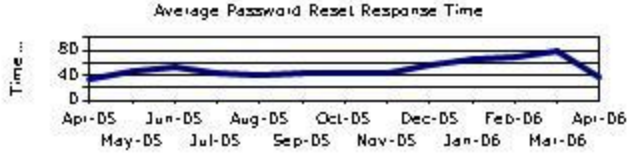


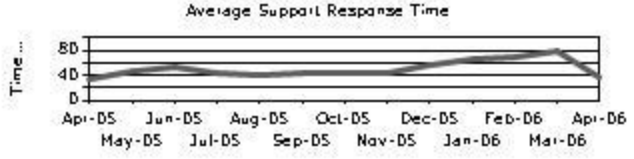
Analysis

Despite the increase in the number of users, there as been a decrease in support costs. This decrease in support costs can be attributed to the decrease in manual password resets.

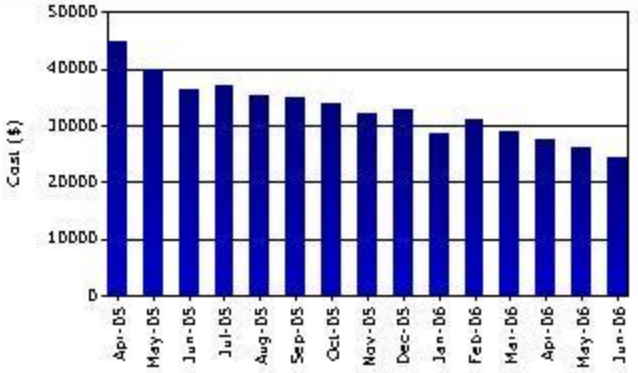
Support Activity







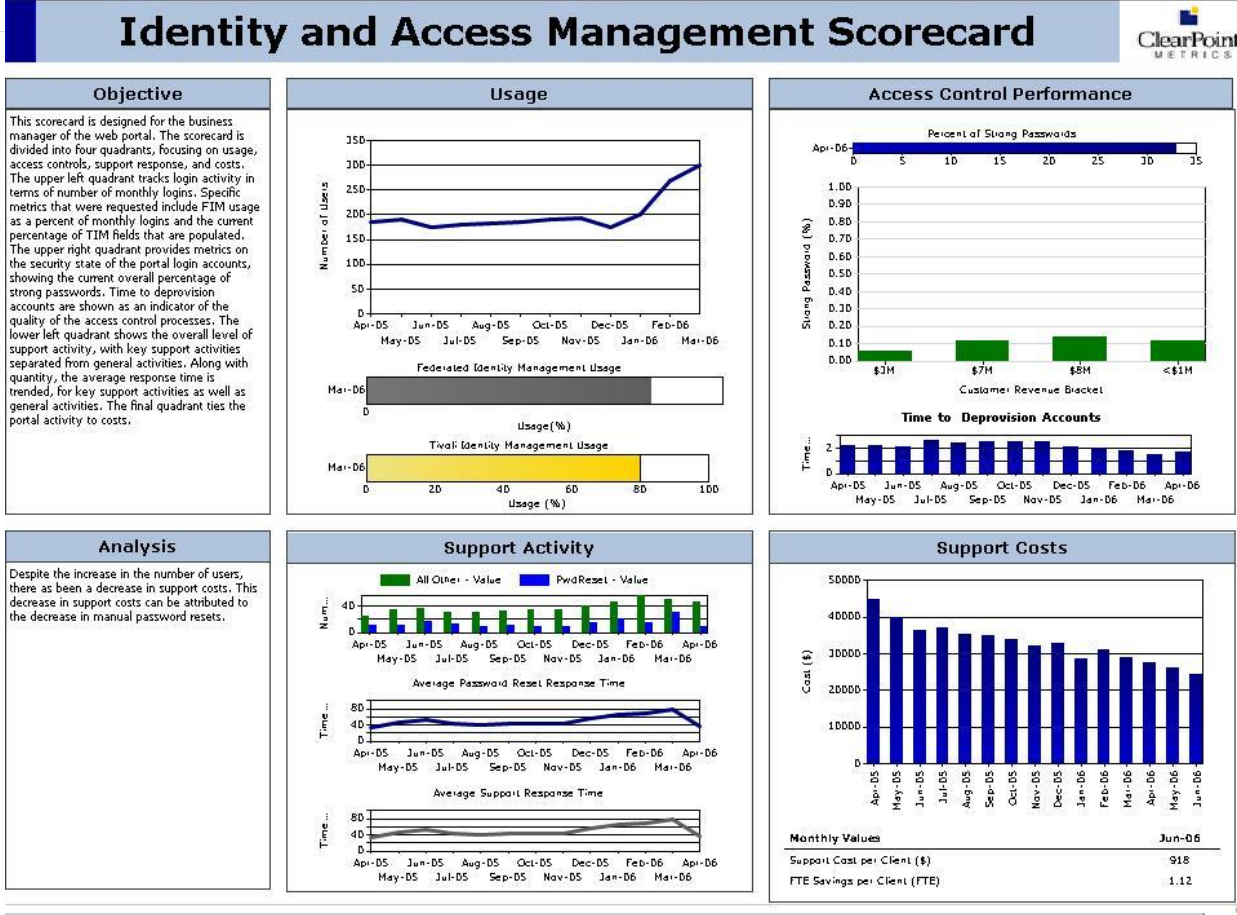
Support Costs



Monthly Values	Jun-06
Support Cost per Client ($)	918
FTE Savings per Client (FTE)	1.12

The two sections on the far left that hold textual narrative provide both a generic description of the information in the scorecard as well as a specific analysis of the data included in this edition of the scorecard. Note that scorecards, in our definition, are regularly published reports. So, for example, a monthly scorecard would have regular editions that are disturbed to entitled consumers precisely once per month—regularly. The analysis of this edition's data appears in the lower left block.

The top middle block is entitled "Usage." The key performance metrics are provided—one with history and two with just the current value. The top graph reflects the count of user accounts that are going through the single sign-on system to access applications. This is a key performance indicator that reflects the adoption rate of the SSO system. It looks like adoption has been accelerating for the past few months. The second two metrics shown in the green and yellow bars reflect first current adoption as a percentage of user accounts and second completeness of user account data in the directory. As we can see, while the raw counts of users leveraging SSO has dramatically risen, we still have a ways to go—over 20% of the user base is still not using SSO. The yellow bar reflects that user information (e.g. title, telephone number, address, etc) is, on average, 80% complete. This is good news for the Customer Resource Management group who will want to develop analytics around application usage and user demographics.



The top right block is designed to reflect Access Control Performance as measured by password strength and time to deprovision user accounts. The top bar indicates what percentage of user passwords are deemed to be "strong" by a password strength rating tool. The green bars break this number down by customer revenue bracket. The low revenue customers seem to have the least strong passwords but the higher revenue customers' passwords are not all that much stronger. One question to consider is whether one should initiate a campaign to educate and/or enforce more stringent password policies. As you will see from the data reflected in the lower left block, this might have a negative effect upon support workload associated with customer password resets. This scorecard provides key insight into the tension between the expense of supporting password problems with customers and the enhanced security of strong passwords.

While the lower left block deals specifically with customer support activity (measured in number of incidents) related to deprovisioning, provisioning and resetting user accounts as measured in number of accounts, the lower right block maps this activity to dollars. It appears that the cost of support is decreasing as a result of increased SSO adoption. Additional metrics could easily be generated to see if the cost of the cost savings in support cover or exceed the cost of the SSO system.

Consumer Web Portal Access Controls

Objective

This scorecard presents key security metrics regarding access control and access related incident responds for an internet facing web portal.

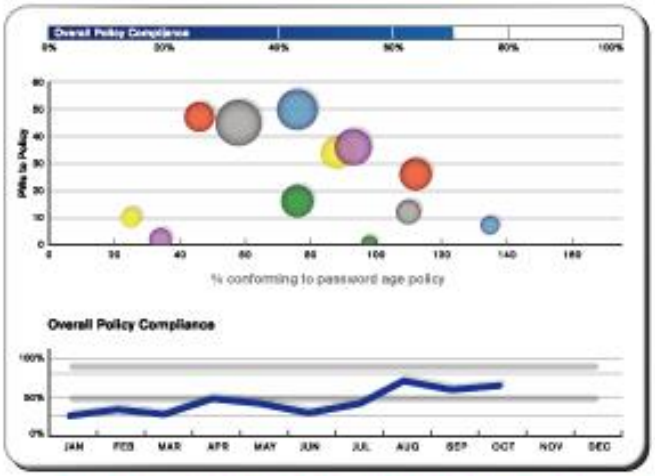
The upper left quadrant shows metrics that characterize both the current and historical states for password policy compliance in terms of password age and strength. The customers associated with bubbles closest to the origin represent the highest risk users.

The upper right quadrant shows current password policy compliance as compared with an established benchmark. Administrator account compliance is highlighted.

Analysis

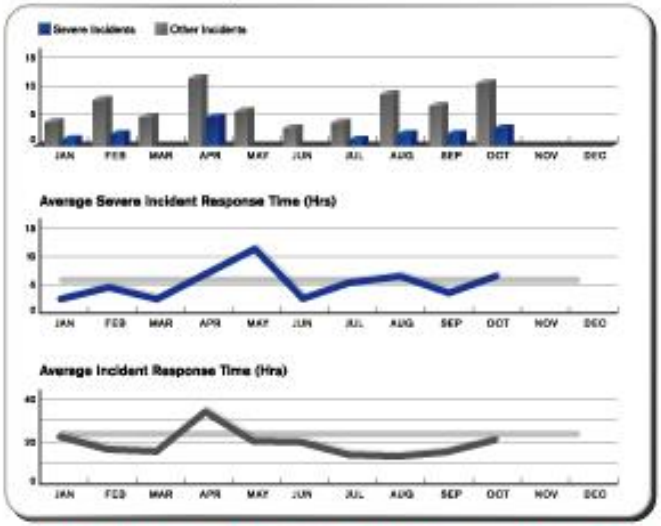
Password strength needs to be improved. We are recommending a targeted training program to increase end user awareness. Another solution would be to modify the password definition software to prohibit weak passwords.

Password Policy Compliance



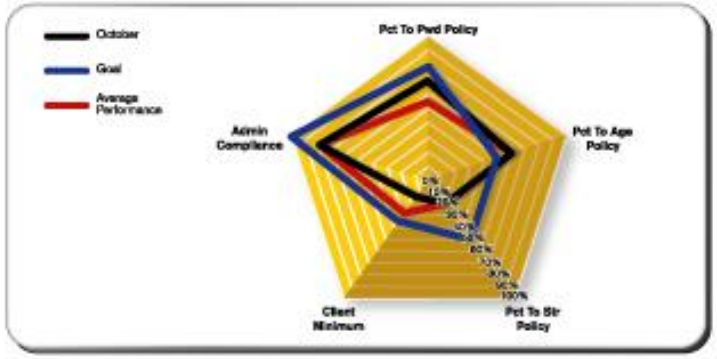
The Operations Group exhibited the poorest performance for password compliance.

Incidents & Response Process



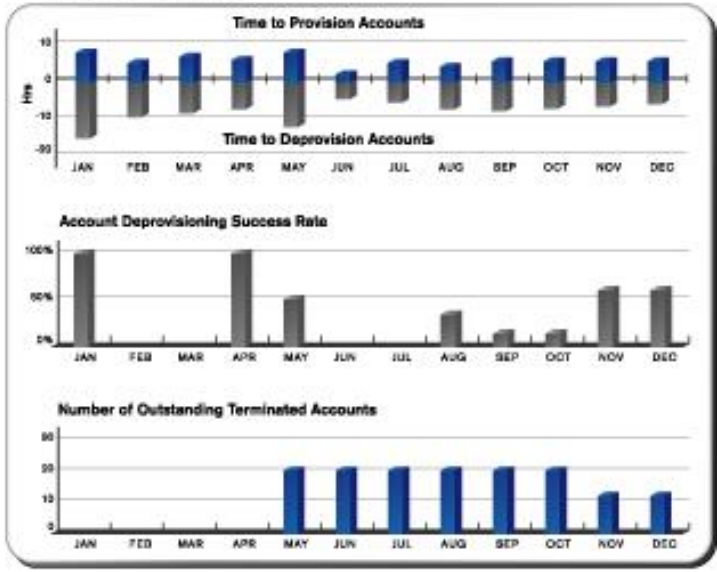
The Security Incident Response Team continues to meet its SLAs for IAM related incidents.

Access Control Performance



Password strength needs to be improved.

Process Quality



Removal of terminated accounts needs improvement. We are continuing to review potential solutions.

Consumer Web Portal Access Controls: Commentary

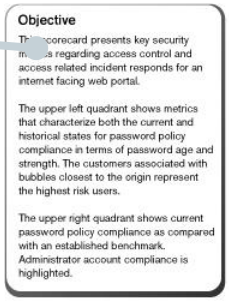
This scorecard presents key security metrics around access controls and access related incidents and responses for an internet facing web portal, enabling a security manager to monitor the state and quality of access controls and processes, and their trends over time.

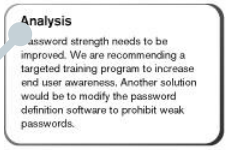
Current State of Passwords

The upper left quadrant shows metrics that characterize both the current and historical states for password policy compliance in terms of password age and strength. The customers associated with bubbles closest to the origin represent the highest risk users.

Objective

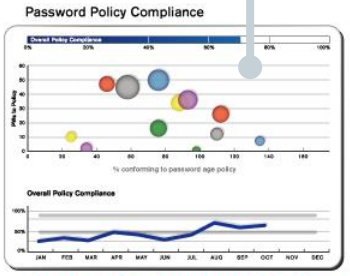
The objective of the scorecard describes the purpose and management goals for the organization's business processes.

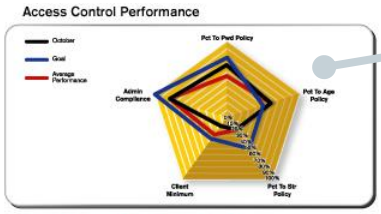




Commentary and Annotation

Space is provided for annotation and comment by the managers involved in this process. The annotation space can be used to explain significant events, changes, or other items of interest.





Multi-Dimensional Detail

The upper right quadrant shows current password policy compliance as compared with an established benchmark. Administrator account compliance is highlighted.

Quality of Access Control Processes

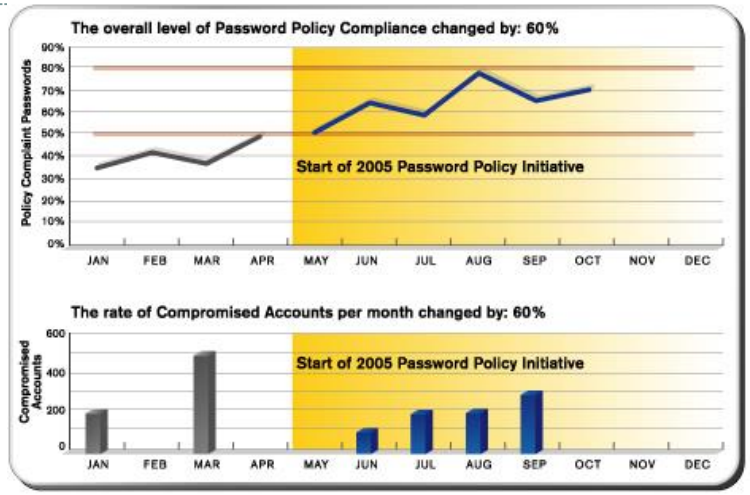
The lower right quadrant captures quality of service metrics for the current reporting period. These include time to provision and de-provision accounts as well as de-provisioning success rate and a raw count of outstanding terminated accounts.

Quality and SLA Levels of Support Response

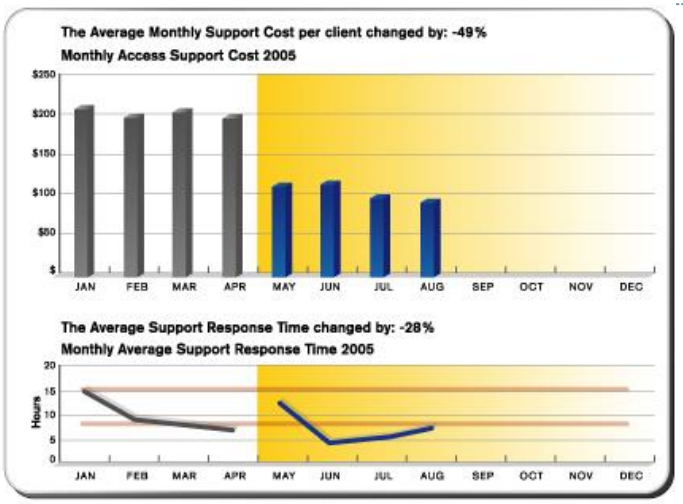
The lower left quadrant characterizes incident frequency and response. Current incident counts as well as historical trends of response times are shown, highlighting these metrics for severe IAM incidents.

Single Sign-on Initiative Value

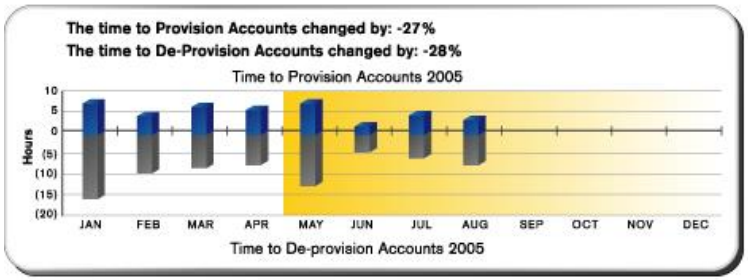
Change in Process Effectiveness



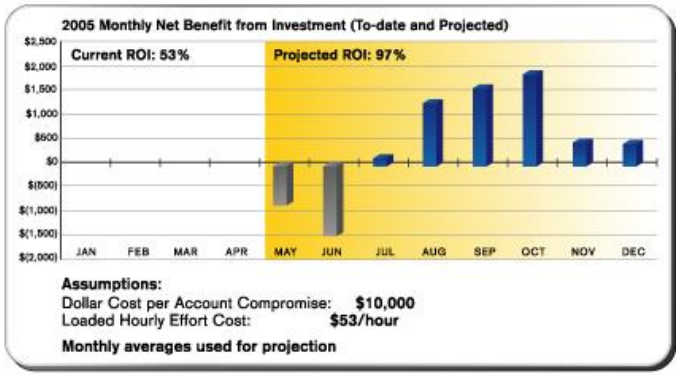
Change in Process Efficiency



Change in Process Quality



Return on Investment



Analysis

The reduction in exposure was validated by the number of incidents experienced and the positive correlation between weak passwords and incidents.

Single Sign-on Initiative: Commentary

The objective of this scorecard is to measure the value, in terms of effectiveness and efficiency, of a specific security initiative to implement a Single Sign-On system. Metrics and charts for effectiveness are on the left hand side. Effectiveness is measured in terms of password compliance, access related incidents, and the time required to provision and de-provision accounts. Efficiency metrics and charts are on the right hand side, and is measured in terms of support workload and effort and a simple ROI calculation.

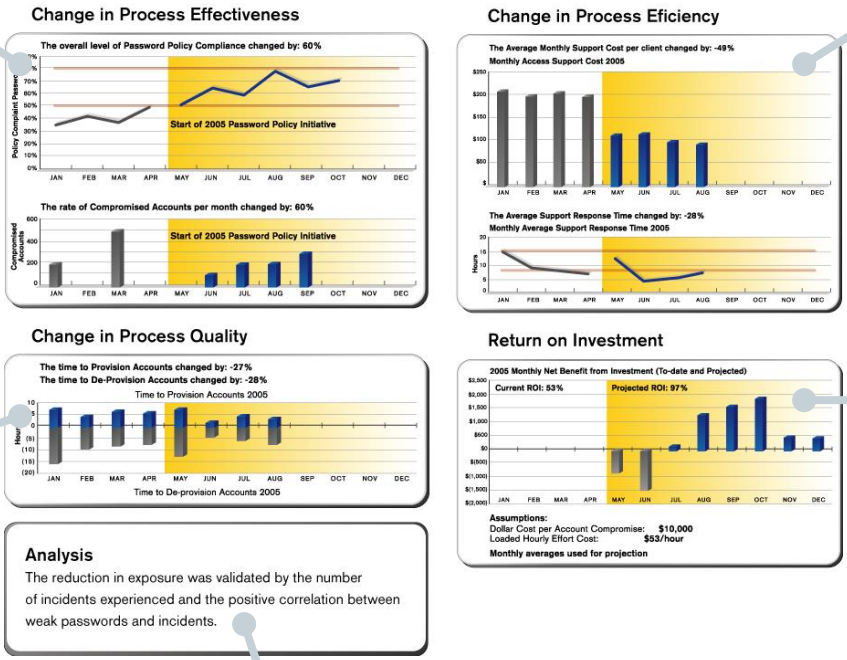
Change in Process Effectiveness

This metric tracks the overall compliance with the password policy.

Correlating Policy adherence with account compromises creates the link between security management activity and security incidents.

Change in Process Quality

The quality of the service delivered is characterized in terms of the effort required to provision and de-provision accounts, both before and after the implementation of the Single Sign-on System.



Commentary and Annotation

Space is provided for annotation and comment by the managers involved in this process. The annotation space can be used to explain significant events, changes, or other items of interest.

Change in Process Efficiency

Much of the benefit of this investment comes from reduced support effort account. In order to complete the picture we need to know if the reduction in cost has come with a reduction in support responsiveness.

ROI

The current return on investment is based on the actual costs and benefits received. Projections are based on the monthly averages and a linear regression model. The simple ROI formula used is:

$$\frac{\text{(Reduction in effort + (reduction in incidents x cost of incidents))}}{\text{(system cost)}}$$

Evaluation

WHAT IS THE BEST WAY TO PRESENT YOUR DATA?

Consider This

How to Present Data for Decisions

- Customers request information in a condensed manner
- A quick “thumbs-up/thumbs-down” view on projects
- Modeled a “star” system similar to mutual fund ratings
- Robots (RAG) are common too

Sample Rating System

- Morningstar for Software Security
- Developing a 5-star/tier rating system
  - Some subtlety of assessment is lost in exchange for ease of use
- Each tier has criteria before a project/measurable may be promoted to the next tier
- Can be applied in a number of ways

Stars Explained

- Absence of Remote and/or Setuid Vulnerabilities

- Absence of Obvious Reliability Issues

- Follow Best Practices

- Documented Secure Development Process

- Passed Independent Security Review

Critique of Rating System

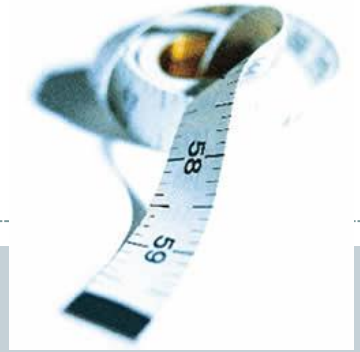
- Ouch!
  - Ratings are very harsh
    - Impact is high for even one exploit
    - If automated tools can find issues, other security defects likely to exist
- Ordering in unordered set
  - The tiered nature implies more importance for some criteria
  - Project information is loss
    - A project may have a defined security process, yet have vulnerabilities present
- Subjectivity of higher tiers
  - Things become more ambiguous as you move up the tiers
    - What qualifies as an independent review?

Using the system

- Can your rating/presentation system allow for questions to be answered ?
  - "Show me 2-star, mid-size, shopping cart software"
- Use stars/coding to filter out components
- Can you drill down to underlying metrics to make a more informed decision on component usage
  - "How does this set of 1-star components compare?"
    - Examine detailed information
    - Does one project have fewer remote exploits?
    - How was this determined?
- Feed metrics into existing risk assessment process to make final determination
  - Model how the selected software will impact existing risk model

Wrapping up

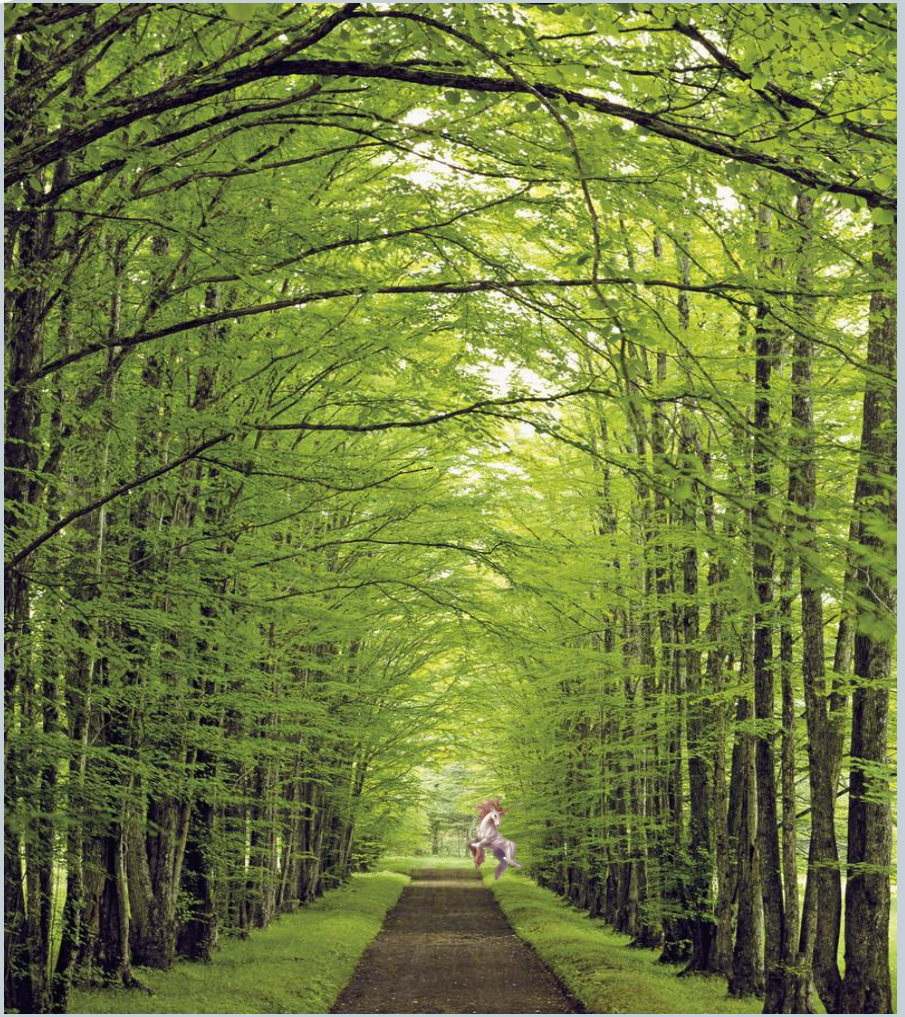
Conclusion



- Be able to answer the following question:
  - *"We are implementing a security metrics program because…"*
- Adhere to measurement best practices
  - Measure what?
  - Why measure it?
  - Measure it for whom?
- Interview key stakeholders to determine what they want
  - Refine into measurable items
- Start with a manageable, useful set of metrics
- Don't forget to set a baseline.
  - Must have to show improvement

Remember ..

- Cant see the wood for the trees.
- Focus on the big picture. Look at the proverbial wood
- Don’t get distracted by the trees (or unicorns)



Remember ..

- Cant see the wood for the trees.
- Focus on the big picture. Look at the proverbial wood
- Don’t get distracted by the trees (or unicorns)