Effective Security Spending: Better metrics allow intelligent spending on security that matters

The current primary focus of information security organizations is the management of operational issues, the supporting tactical projects, and maintaining of compliance activities. The development of a metrics framework enables a proactive approach to security management utilising security information to inform strategy, compliance, service management and efficiency. Clear metrics enable the communication of the business benefits of security and will assist in obtaining stakeholder support. HP Enterprise Security will discuss their framework and tools for establishing metrics as well as what is seen as best practice in major organizations globally. They will show how to practically achieve a metrics programme.
The Business Problem

With an ever increasing focus on operational costs and risk, organisations are demanding a more transparent Enterprise Security Programme.

Considerations include:

• Focus on Security Programme Performance Measurement.
• Requirement for data that can be used to measure Cyber Efficiency.
• Disclosure of a variety of security metrics that relate to business goals and KPIs.
Business Demands

Typical Requirements:

- What is the Organisational Security Status on a day-to-day basis?
- How can I use Security Metric Trends to enable effective Security Monitoring and Budget spend?
- How can I use automation to reduce IT Security Risk across the organisation?
- How can I benchmark the organisation against best practice and industry peers?

At a technical level, using SPAM metrics as an example:
- How many emails came into the Gateways today?
- How many were deleted there and then (deleted/dropped based on confidence levels that they were SPAM)?
- How many were quarantined?
- How many were released from quarantine by staff?
  - One customer saw an opportunity to reduce staff costs in dealing with quarantined emails
  - The customer asked for the filters to be tightened to delete more at Gateway until people started to complain
  - The risk was underwritten by the customer, not HP
HP - Protecting the extended enterprise

HYBRID SECURITY INFRASTRUCTURE

- **Data Center**
  - E-Mail Security
  - Database Security
  - Web/URL Filtering
  - Cloud Infrastructure Security

- **Network**
  - DLP – In Motion
  - IDS/IPS
  - Secure Perimeter
  - Network Access Control

- **Apps & Data**
  - DLP – In Use
  - Web Application FW
  - Application Vulnerability Scanning
  - Secure Application Development & Delivery

- **Users & Devices**
  - DLP – At Rest
  - Enterprise Mobile Security
  - Endpoint Protection
  - Encryption

Governance, Risk and Compliance (GRC)

- Security Strategy
- Risk
- Policy
- Architecture & Standards
- Compliance & Audit
- Performance Metrics

Security Operations & Intelligence

- OP Sec
- Monitoring
- TVM
- Incident Response
- IAM
- BCRS

SECURITY SERVICE MANAGEMENT (SSM)

- SSM SLAs & Metrics
- SSM Control Framework
- SSM Hub
Security Metrics – HP PoV

Metrics - derived from specific business goals and objectives.

Goal-Objective-Metric Hierarchy

- **Goals**
  - Business targets that are underpinned by a set of objectives.

- **Objectives**
  - Specific activities that deliver goals.

- **Metrics**
  - Data that can be used to measure objectives.

Metrics Hierarchy Definitions
Security Metrics - Characteristics

Qualities of good metrics
1. Linked to Business Goals
2. Controllable
3. Low Overhead
4. Quantitative (Nominal, Interval, Ordinal, Ratio)
5. Trendable

Good metrics practices
1. Must be Targeted to Audience
2. Must be Hierarchical
3. Must be Actionable
4. Frequency should be tied to reality
5. Support Continuous Improvement
The collection and analysis of security metrics should be bounded by a number of phases that provide data input to the security programme.
Joining it up - Cyber Defence solution

STAKEHOLDERS

- Employees
- Customers
- Vendors
- Management
- Businesses
- Functions

PARTNERS

- Information Security
- Physical Security
- I.T. Operations
- Privacy
- Audit
- Communications
- Public Relations
- Legal
- Help Desk
- Operations
- Global Network Operations
- HR / ER

OTHER

- Citizens
- Law Enforcement
- Intelligence Sources
- Third-parties

PROGRAM AREAS

- Threat Analysis
- Vulnerability Detection
- Malware/AV
- Patch Management
- Counter-measures
- Investigations & Forensics
- Network / Host Security Management
- Identity & Access Management
- Compliance & Security Monitoring

Escalation & Crisis Management

- Incident Response Team
- Program Administration, Analysis & Reporting
- Program Rollout & Awareness

Corporate Crisis Management Team

IT & Information Security Management Teams
HP Security Metrics Framework

HP has developed a comprehensive Security Metrics Framework based on phases of a security programme versus stakeholder types. Indicators are defined at four Phases:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Security Operations</th>
<th>Plan Management</th>
<th>Business Stakeholders</th>
<th>External Stakeholders</th>
</tr>
</thead>
</table>
## Security Metrics Framework

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Govern</td>
<td>Operational Risk Data</td>
<td>Efficiency and Effectiveness</td>
<td>Risk Exposure</td>
<td>Risk Exposure</td>
</tr>
<tr>
<td>Plan</td>
<td>Plan Data</td>
<td>Plan Status</td>
<td>Plan Effectiveness</td>
<td>Plan Effectiveness</td>
</tr>
<tr>
<td>Build</td>
<td>Compliance Data</td>
<td>Compliance Status</td>
<td>Compliance Status &amp; Trends</td>
<td>Compliance Status</td>
</tr>
<tr>
<td>Run</td>
<td>Service Management Data</td>
<td>Service Status</td>
<td>Service Trends &amp; ROI</td>
<td>Service Availability</td>
</tr>
</tbody>
</table>
Security Metrics – The Big Picture

Security Dashboard

<table>
<thead>
<tr>
<th>Threat Mgt</th>
<th>Risk Mgt</th>
<th>Policy Mgt</th>
<th>Compliance Mgt</th>
</tr>
</thead>
</table>

Output

SECURITY METRICS FRAMEWORK

Input

Threat Intelligence

SIEM

SOC Tools

Network Configuration

Infrastructure Management

Security | DB | Server | Network

Apps & SMDB

BIA Data

Business Process Information

Policies

Policy Information

Configuration Data

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Security Metrics Approach

Project Initiation
• Definition of project plan, SoW, milestones, deliverables.

Pre-Workshop
• Stakeholder interviews.
• Review current metrics programme
• Gap analysis with HP’s Security Metric Framework

Workshop
• Review and validate the business objectives, control layers and audiences.

Analysis
• Categorisation of metrics
• Alignment with Stakeholders and business objectives

Metric Framework Report
• Catalogue of metrics
• Road map implementation recommendations
Standard Metrics Catalog

Inventory (Asset Count)
- People: Users, security FTEs
- Equipment: Desktops, servers, network devices, security devices
- Resources: connections, applications

Program Status (Against Planned Objectives)
- Percent YTD spending of security budget
- Percent completion of annual objectives
- Percent confidence of completing objectives
- Percent security policies refreshed
- No. of policies reviewed, created, implemented
- No. of security processes defined, matured (and level)

Project Status (Major, per Project)
- Percent completion
- Percent project timeline elapsed
- Percent project budget expended
- Percent confidence of completion

Audit and Regulatory Compliance
- No. of compliance deficiencies, last audit
- No. of remaining open compliance deficiencies
- Y/N compliance audit up-to-date
- No. of policy deficiencies, last audit
- No. of remaining open policy deficiencies
- Y/N policy audit up-to-date
Standard Metrics Catalog Cont.

Event/Incident Management
- No. of privacy violations
- No. of events (total, reportable, ability to be investigated, actionable)
- No. of hours induced downtime by system criticality.
- No. of incidents by type (configuration error, zero-day vulnerability, unpatched vulnerability, user error, hacker)

Security Systems Status/Health
- Percent desktops with fresh AV
- Percent of FW/IDS/VPN/etc. with fresh firmware
- Percent availability of security infrastructure

Communications/Awareness
- Percent users "made aware" during period
- Percent IT personnel trained during period

Risk Assessment Status
- No. of risk assessments conducted
- No. of risk assessments in progress
- No. of risk assessments pending or backlogged
- No. of critical systems with expired RA

Vulnerability Management (Includes Patch)
- No. of security alerts processed
- No. of vulnerability scans in period
- No. of open vulnerability by criticality
- No. of vulnerability reduction during period (area, volume)
Standard Metrics Catalog Cont.

Service requests
  • Change requests for security review (approved/rejected/appealed)
  • Application development/acquisition security reviews requested/completed
  • New user requests (staff addition)
  • User move/add/change (normal/exception)
  • New role definition requests
  • Role definition change requests
  • Delete user requests (normal/urgent)
Service Management Context

Security Management

- Continuity Management
  - Security specifications for continuity plan
- Capacity Management
  - Capacity Reports
- Service Planning
  - Service Design
- Service Build and Test
  - Security specifications for new services
- IT Strategy and Architecture Planning
  - Security Specifications for architecture design
  - IT Architecture
- Configuration Management
  - CI Attributes and Relationships
- Availability Management
  - Exception Approvals
- Problem Management
  - Assessment
  - Security Plan, OLAs
  - Security Specs
- Operations Management
- Service Level Management
  - Security section of SLA's
- Change Management
  - Security Plan
- Incident Management
  - Trigger security incident response

Process trigger
The HP Metrics Journey

- Security Metrics Framework
- Information Assurance Dashboard
- Security Analytics

Summary Chart against existing benchmark:
- Current Benchmark Capability
- Your Current Capability Maturity
- Target Benchmark Capability
- Your Target Capability Maturity

Strategy vs. Compliance vs. Infrastructure vs. Issue
Security Programme - Maturity Model

Phases of Maturity

- Blissful ignorance
- Awareness
- Corrective
- Operations excellence

Maturity Level

Relative Maturity Level

Non-Existent Risk

Initial Developing Defined Managed Optimised

Security Metrics Framework
Information Assurance Dashboard
Security Analytics

Informatio

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
IA Security Dashboard Overview

• Centralised view across the Enterprise

Features:
• Simple and easy to use interface
• Secure web access
• Integration with software such as SIEM tools
• Benchmarking capabilities
• Clear, accurate and meaningful reporting

Problem it solves:
• Enterprises often lack an overall view of their security operations, risk, compliance and budget creating difficulty in making informed business risk and security decisions

Benefits:
• Gives a total view of enterprise security, based on security metrics.
• Aggregates metrics from multiple systems for reporting.
• Aligns information security to business strategy to address risk.
• Improves control of security programme.
Security Analytics

Explore Decisions and their Effects on KPIs.

• Explore the effects of different models and solutions to a Security Process, Technology Implementation or Transformation.
• Discover the most Effective security solution for the right level of investment.

Provide Evidence to Support a Business Case

• Empower the CISO to gain stakeholder support by providing evidence of the outcome of proposed investments.
• Provide vital input into the investment decision logic.

Explore the Sensitivity of a Security Programme to Change.

• What if-
  • The number of threats doubles next year, will our Cyber Security defence be resilient?
  • If we change a Security Process, what impact will this have on the Security and other audiences?
HP PoV – Security Metrics

- Security Leaders need to understand that they are deriving maximum value out of the IT and Security budgets, and require the data that can be used to measure Cyber Efficiency and align with KPIs.
- Business leaders have a vested interest in Security Programme Performance, and are demanding the disclosure of a variety of security metrics that relate to specific business roles.
- There is a lack of security related data to support both internal and external risk and audit teams.
- There is an overarching need for security to evolve and manage risks associated with organisational changes, including disruptive changes such as mergers, cloud and virtualisation.

A well defined metrics framework enables the measurement and communication of security programme effectiveness and its impact on business objectives.
Thank you