Metrics that Matter

SANAZ SADOUGHI
INTERNATIONAL MONETARY FUND
The views expressed herein are those of the speaker and should not be attributed to the IMF, its Executive Board, or its Management.
Who We Are and Why Do We Care?

189 member countries
Lending
Capacity
Development
Surveillance
Uneasy Questions

- How secure are we?
- What is our information security posture today compared to last quarter?
- Do we need to invest more in our current capabilities and people?

- How effective are our controls?
- What are our threats and high risk areas?
- Are we protecting the most valuable assets?
- What is the level of compliance to our security policies?

- Where should we allocate our resources to address high risk areas?
- Are we meeting our SLA’s in addressing incidents and patching?
Multiple systems of information

Data collections / cleansing

Manual processing

Manual analysis

Silo reporting

Lagging and leading indicators

Relevant

Impactful

Actionable

Different audiences

=
Our Goal

Where we are & How we Progress

- Track & manage risks
- Reduce risk
- Support risk trade-off decision making

How to Prioritize Decision Making

- Report on outcome of security investments
- Set targets for performance improvement & monitor
- Help with decision making

How to Answer to Questions

- Provide evidence of risk management & compliance
- Underpin risk appetite discussions
- Satisfy stakeholder expectations
- Make the case for funding
Our Proposed Vision

**Business Value**
- Answers leadership questions
- Transparency
- Context to communicate better
- KRI

**Operational Value**
- Provides self-service platform that enables decision-making.
- Drives cyber hygiene improvements and adds value.
- KPIs measured by SLAs
- Provides drill-down capability
- Uses available data in our environment
Overview of the Information Security Metrics Program (ISMP)
Where Are We Today

- Metrics on 7 domains
- Using 21 source systems
- Monthly reports
- CIO, CISO, Operational Teams, ERM, Audit
How to Start

Define Requirements
- Identify business objectives
- Questions to be answered

Identify Data Sources
- Assets
- Data owners

Data Collection
- Data validation
- Data cleansing
- Data correlation

Analysis
- Based on agreed approach
- Drill-down
- Consolidated not only silos
- Repeatable

Reports
- Focus on story
- Make it interactive
- Dashboard
- Most important metrics
Objectives of the ISMP

The Implementation of an Information Security Metrics Program (ISMP) allows the organization to:

- Effectively communicate security posture
- Demonstrate the value of the security investment
- Drive performance improvement
- Help prioritize decision making
- Manage risk and compliance
- Provide quantitative measurements
The ISMP Framework

The stakeholder questions can be answered through an ISMP framework below:

Scope of metrics and data collection

Source 1  Source 2  Source ...  Source n

Metrics (Context, KPIs & KRI)

Domain 1  Domain 2  Domain ...  Domain n

Dashboard & Reports

Governance & On-going Maintenance

Information Security Metrics Program Outcome

Return on Investment  Risk & Compliance Management  Trending & Set Targets

Data Collection

Analysis & Metrics

Dashboard

Story
The metrics catalog has been designed based on the following hierarchy:

Domain → Outcome → Metric → Raw Data

Vulnerability Management → Understand threat/vulnerability → % of High vulnerabilities → # of critical vulnerabilities

Vulnerability Management → Understand threat/vulnerability → % of Critical vulnerabilities → # of vulnerabilities
## Domains & Reporting

### Domains

<table>
<thead>
<tr>
<th>1. Security Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Vulnerability Management</td>
</tr>
<tr>
<td>3. Compliance Management</td>
</tr>
<tr>
<td>4. Risk Management</td>
</tr>
<tr>
<td>5. Identity &amp; Access Management</td>
</tr>
<tr>
<td>6. Threat &amp; Incident Management</td>
</tr>
<tr>
<td>7. Security Technologies</td>
</tr>
</tbody>
</table>

### Reporting Structure

- **IMF Mgmt., Board** (Annual)
- **CIO, CISO, ERM, Audit, Operational Mgmt.** (Quarterly)
- **Operational Teams** (Monthly)
Program Level Dashboard

These reports will be reviewed on a monthly basis to take action.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Domain Score</th>
<th>Domain Target Range</th>
<th>KPI - KRI</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Security</td>
<td>3.4</td>
<td>3.5 – 4.0</td>
<td>KRI (effectiveness of Investment)</td>
<td>Growth</td>
</tr>
</tbody>
</table>

Top Performing Metrics
- % of mobile devices managed via MDM: 100%
- % of mobile devices encrypted: 100%
- % of mobile devices with MDM disabled: 0.3%

Bottom Performing Metrics
- % of mobile devices running iOS version 7.x: 23.4%
- % of mobile devices non-compliant with mobile security policy: 10.8%

EXAMPLE ONLY
Revised Metrics & KRI's

Tailored to audience and Agreed on what's important - Iterative testing of what works
Measure Security Posture Using NIST CSF

Adopt and customize NIST Cybersecurity Framework (CSF) which relies on variety of standards, guidelines.

1. Define the current and target security maturity postures
2. Define KRI, thresholds, reporting frequency
3. Drive Action

Desired information security posture
Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

<table>
<thead>
<tr>
<th>Function</th>
<th>Domain/Category</th>
<th>Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect (DE)</td>
<td>Anomalies and Events</td>
<td>2.9</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>2.2</td>
</tr>
</tbody>
</table>

### Domain

- **Vulnerability Management (Detection Processes)**
  - % of critical vulnerabilities on **most-exposed** infrastructure: < 5% < 10% < 20% >= 20%
  - KRI Score: 4
  - % of critical vulnerabilities on **internal** infrastructure: < 25% < 50% < 75% >= 75%
  - KRI Score: 3

### Risk Statement

Vulnerabilities in the assets can be exploited & led into information disclosure, financial loss, etc.

### Proposed Actions

Remediate critical vulnerabilities
Crown Jewels

Create metrics dashboards for Crown jewels:
  ◦ Identify the sensitive information assets
  ◦ Identify the most critical infrastructure and applications

Prioritize vulnerability assessment and remediation

Prioritize compliance assessment and remediation
Demo of Metrics & Dashboards
Demo of User Behavior Analysis

EXAMPLE ONLY
IMF Next Steps

- Automation and reduce overhead
- Focus more on context and analysis
- Stakeholder iterative input to refine KRI’s
- Align to NIST CSF (quantitative and qualitative) measures
- Report on actions taken and impact
Next Steps – How you to Apply

**Next Month:**
- Identify your organizations’ key questions
- Define your requirements and what resonates with your audience

**In the first 3 Months:**
- List your data sources
- Define potential metrics to start with

**Within 6 Months:**
- Create sample reports
- Identify quick wins
Thank You!

Sanaz Sadoughi

sskhosroshahi@imf.org

International Monetary Fund