Cybersecurity Metrics

Supporting accurate and timely decision-making

November 2018

Anthony Muiyuro
Cybersecurity Leader, EY East Africa.
## Business drivers

While more questions are being asked about cybersecurity, current reporting is not adequate.

## Challenges

Organizations are struggling to determine what and how to report on cybersecurity.

## Building an Effective metrics program

Improve cybersecurity reporting requirements.

## The CISO Dashboard
"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
Business drivers
It can be challenging to communicate the value of Cyber Security in business terms

- Are our security investments paying off?
- How secure is our organization?
- How well are we identifying and responding to relevant threats?
- Is our security program on track to achieve maturity objectives?
- How do we continue to get support for cyber security efforts from executive leadership?
- Are our response capabilities adequately managing the impact of incidents to the organization?
- Are cyber security services delivered in a fashion that meets business needs?
- How does a CISO defend the cyber security budget?
- As the focus on cyber security has continually increased, Information Security functions are faced with a number of difficult questions.
Telling “the Cyber Security story” is complicated for many reasons

- **Lack of common language**: Information Security lacks a mature common language to describe its complex environment in terms of business value.

- **Difficulty in obtaining required data**: Consistent, timely and relevant data to support reporting often is not readily available.

- **Organizational differences**: Varying Information Security organizational structure and responsibilities make it difficult to standardize reporting focus areas.

- **Lack of performance baselines**: There are no established widely accepted performance baselines.

- **Legacy thinking**: Legacy approach to security reporting is focused on tracking what is being done vs. how well it is being done.

**Most traditional ways of reporting focus on available data rather than the needs of the reader**
Stakeholders to ‘Manage’

- Is the cybersecurity strategy aligned with our business strategy?
- Are security initiatives on track to remediate risks and improve security?
- Is the organization complying with policies and regulations?
- Is the money spent on cybersecurity creating value?
- How efficient have our tools been in protecting against cyber attacks?
- Do we have real-time insights into critical incidents, threats and vulnerabilities impacting our environment?
- What are our key risks and how can we mitigate them?
- Do we have appropriate and effective controls in place?

Roles:
- Chief Executive Officer
- Functional Leads
- Chief Compliance Officer
- Chief Information Security Officer
- Chief Risk Officer
- Internal Audit
- Chief Information Officer
- Board
Organizations are struggling to determine what and how to report on cybersecurity.

<table>
<thead>
<tr>
<th>Cyber threats are just one of the many risks that organizations face. Most organizations struggle with fully understanding what they need to report on and to whom (e.g., to boards, audit committees)</th>
<th>Cybersecurity metrics are often presented as key risk indicators or key performance indicators that are accurately measurable; however, these often tell “nothing but the truth,” but not the “whole truth” as they lack business context.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing cybersecurity, governance risk and compliance (GRC), and service management technologies increasingly have dashboard and reporting capabilities but are often not integrated.</td>
<td>Legacy approach to security reporting is focused on tracking what is being done versus how well risk is being reduced. As a result, current reporting does not provide the insight needed to take risk-based business decisions.</td>
</tr>
<tr>
<td>Many executive cyber reports are largely manually compiled on an ad-hoc or inconsistent frequency and require significant effort and time to produce.</td>
<td>Existing reporting often lack actionable information that can be used to remediate issues quicker and more effectively.</td>
</tr>
</tbody>
</table>
Developing an Effective Metrics Program
Well designed metrics support decision making

**INFORMATION = DATA + VALUE + CONTEXT**

- **Right information**
- **In the right format**
- **At the right time**

**Decision support**

- **Response capabilities**: Decisions that take into consideration both external and internal factors and demonstrate response capabilities.
- **Strategic alignment**: Decisions that strategically align with organization’s vision and objectives.
- **Operational excellence**: Decisions that maximize operational efficiency and effectiveness.

**INFORMATION = DATA + VALUE + CONTEXT**
Three categories of security measures are critical in enabling decision making

<table>
<thead>
<tr>
<th>Reports…</th>
<th>Answers…</th>
<th>Supports…</th>
<th>Characterized as…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress enabled with context from the broader Cyber Security program (e.g., counts, percentages, forecast to actual, burn rate, etc.)</td>
<td>Technical data contextualized against internal and external relevant factors</td>
<td>Processes evaluations against performance objectives (e.g., timeliness, quality, consistency, effectiveness, etc.)</td>
<td></td>
</tr>
<tr>
<td>What are we doing? (security projects &amp; initiatives)</td>
<td>Are we doing enough? (security controls)</td>
<td>Strategic alignment and Operational excellence</td>
<td>Time-bound and Outcome-based</td>
</tr>
<tr>
<td>How well are we doing? (security processes)</td>
<td></td>
<td>Response capabilities</td>
<td>Outcome-based</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operational excellence</td>
<td>Outcome-based and Quality-focused</td>
</tr>
</tbody>
</table>

Supports…
- Strategic alignment
- Operational excellence
- Response capabilities

Characterized as…
- Time-bound
- Outcome-based

Strategic alignment and Operational excellence
- Outcome-based
- Quality-focused
Maturity Goal
Organizations cannot wait until they have reached their desired maturity to begin measuring security.

Many Cyber Security organizations erroneously opt to delay implementation of performance management programs in order to allow their functions to mature. This approach puts underdeveloped and unsophisticated cyber security organizations at greater risk of not getting the attention and investment they need to transform and develop as they lack the metrics and measurements necessary to demonstrate their value to the overall business as well as the gaps that exist.

Security performance management enables organizations to improve within and across maturity levels:

<table>
<thead>
<tr>
<th>INITIAL</th>
<th>REPEATABLE</th>
<th>DEFINED</th>
<th>MANAGED</th>
<th>OPTIMIZING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics can help identify high-risk areas for targeted improvement and support funding requests for larger efforts by providing visibility into “security” gaps.</td>
<td>Metrics can assist in obtaining visibility into some basic repeatable processes while driving performance to desired levels.</td>
<td>Metrics can assist in the formalization of security functions and services by quantifying performance expectations and reporting on progress.</td>
<td>Metrics can be used to effectively report on the performance of operational activities and the quality of services delivered.</td>
<td>Metrics can drive continuous security program enhancements and performance improvement towards strategic goals.</td>
</tr>
</tbody>
</table>
Improving cybersecurity reporting requirements.
Cybersecurity reporting should enable accurate and timely decision-making

Reporting must:
- Provide a realistic view of cyber risk posture
- Be readily available and produced consistently for all stakeholders
- Demonstrate analysis, knowledge and expertise

- Critical incidents
- Risk posture/trend
- Spend status/ROI
- Compliance

- Portfolio status/health
- Financial and organizational health (e.g., budget, headcount)

- Control health (e.g., patching, malware protection)
- Mapping to controls (e.g., NIST, ISO)
- Project status/health

- Operational risk (e.g., incidents, threats, vulnerabilities)
- Activities status
Improving the maturity of your cybersecurity reporting

Fig. Maturity model for cybersecurity reporting

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Ad hoc metrics; created only when requested.</td>
</tr>
<tr>
<td></td>
<td>Manual dashboards (e.g., Excel, PowerPoint).</td>
</tr>
<tr>
<td></td>
<td>Highly manual effort.</td>
</tr>
<tr>
<td>Repeatable</td>
<td>Tactical metrics focused on select security domains.</td>
</tr>
<tr>
<td></td>
<td>Manual dashboards created at some regular frequency.</td>
</tr>
<tr>
<td></td>
<td>Effort still largely manual.</td>
</tr>
<tr>
<td></td>
<td>Metrics may be influenced by industry frameworks.</td>
</tr>
<tr>
<td>Managed</td>
<td>Strategic and tactical metrics, KPIs* and KRI*s to monitor coverage and effectiveness.</td>
</tr>
<tr>
<td></td>
<td>Dashboards leveraged for decision-making.</td>
</tr>
<tr>
<td></td>
<td>Mostly automated dashboard; very limited manual effort.</td>
</tr>
<tr>
<td></td>
<td>Most metrics pulled from source system in near real-time.</td>
</tr>
</tbody>
</table>

*NIST - National Institute of Standards and Technology
*ISO - International Organization for Standardization
*KPI – Key Performance Indicator
*ISO – Key Risk Indicator
Cybersecurity dashboards can help provide tangible contributions to the organization.

- Near real-time* insights into critical threats and incidents
- Increased visibility into risk posture and control gaps
- Predefined profiles to target specific organizational roles
- Customizable dashboard and reports to suit various reporting needs
- Integrated and consolidated cyber dashboards
- Graphic and visual representation of actionable insights

*Depending on availability of data and capability of organizational tools
Developing a systematic framework to create relevant, comprehensive, automated dashboards.

Metrics should be part of the life cycle with continuous assessment and improvement steps. The output has direct impact for a business from financial to risk reduction.
Demo dashboard: CISO executive overview

Target audience: CISO and the leadership team
Objective: cover key operational, controls health and project status metrics
Demo dashboard: CISO executive overview

Target audience: CISO and the leadership team

Objective: cover key real-time operational metrics for daily usage
Demo dashboard: business unit overview

Target audience: business unit IT leaders
Objective: highlight cyber risks for applications tied to a business unit and what risks to focus on first
Demo dashboard: cyber operations

Target audience: CISO and the leadership team

Objective: key metrics on incident, threat and vulnerability management
Demo dashboard: CISO overview mobile view

Target audience: CISO and the leadership team

Objective: Key operational metrics
Let's Discuss..............
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Advisory Services
EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

The better the question. The better the answer. The better the world works.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no: 01799-183GBL
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com