Cybersecurity Metrics

Supporting accurate and timely decision-making

November 2018

Anthony Muiyuro
Cybersecurity Leader, EY East Africa.

Building a better working world

Contents

Metrics story

"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

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’

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

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)

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.

Existing cybersecurity, governance risk and compliance (GRC), and service management technologies increasingly have dashboard and reporting capabilities but are often not integrated.

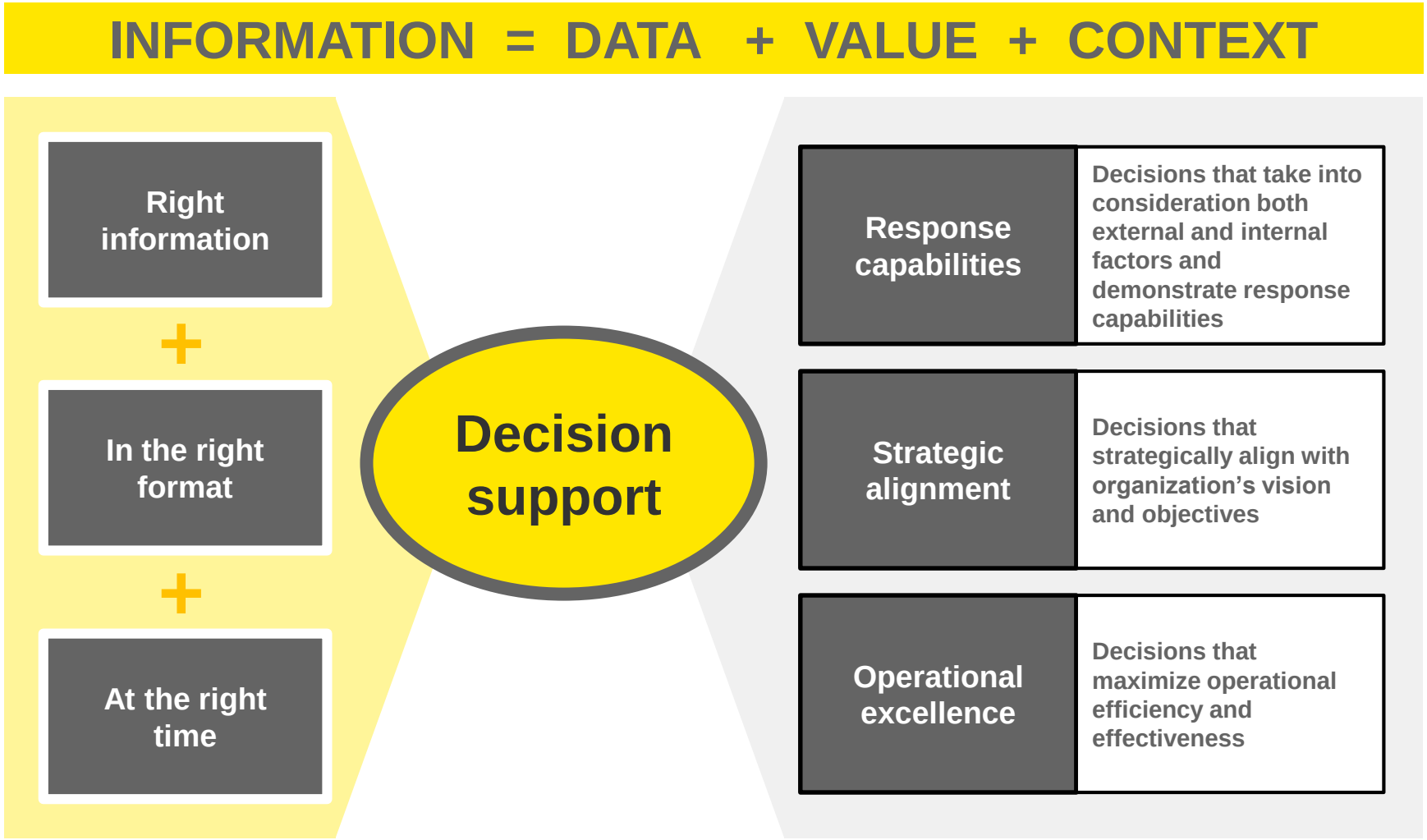
Legacy approach to security reporting is focused on tracking what is being done versus how well risk is being reduced. As a result, current reporting does not provide the insight needed to take risk-based business decisions.

Many executive cyber reports are largely manually compiled on an ad-hoc or inconsistent frequency and require significant effort and time to produce.

Existing reporting often lack actionable information that can be used to remediate issues quicker and more effectively.

Developing an Effective Metrics Program

Well designed metrics support decision making



Three categories of security measures are critical in enabling decision making

	Relative State of IS Program Progress	Relative State of Security Posture	State of IS Operations Performance
Reports…	**Progress enabled with context from the broader Cyber Security program (e.g., counts, percentages, forecast to actual, burn rate, etc.)**	**Technical data contextualized against internal and external relevant factors**	**Processes evaluations against performance objectives (e.g., timeliness, quality, consistency, effectiveness, etc.)**
Answers…	**What are we doing?** *(security projects & initiatives)*	**Are we doing enough?** *(security controls)*	**How well are we doing?** *(security processes)*
Supports… • Strategic alignment • Operational excellence • Response capabilities	**Strategic alignment and Operational excellence**	**Response capabilities**	**Operational excellence**
Characterized as…	**Time-bound and Outcome-based**	**Outcome-based**	**Outcome-based and Quality-focused**

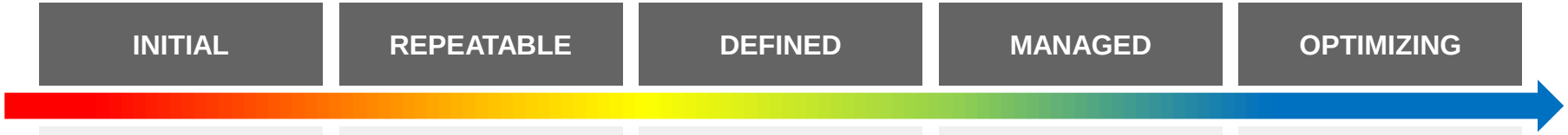
Maturity Goal

Organizations cannot wait until they have reached their desired maturity to begin measuring security

Good metrics drive change

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



INITIAL	REPEATABLE	DEFINED	MANAGED	OPTIMIZING
Metrics can help identify high-risk areas for targeted improvement and support funding requests for larger efforts by providing visibility into “security” gaps	Metrics can assist in obtaining visibility into some basic repeatable processes while driving performance to desired levels	Metrics can assist in the formalization of security functions and services by quantifying performance expectations and reporting on progress	Metrics can be used to effectively report on the performance of operational activities and the quality of services delivered	Metrics can drive continuous security program enhancements and performance improvement towards strategic goals

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

*NIST - National Institute of Standards and Technology

*ISO - International Organization for Standardization

*KPI – Key Performance Indicator

*ISO – Key Risk Indicator

Initial

- Ad hoc metrics; created only when requested.
- Manual dashboards (e.g., Excel, PowerPoint).
- Highly manual effort.

Repeatable

- Tactical metrics focused on select security domains.
- Manual dashboards created at some regular frequency.
- Effort still largely manual.
- Metrics may be influenced by industry frameworks.

Defined

- Metrics cover most security domains.
- Metrics provide high-level view of security risk across the enterprise.
- Dashboard development is operationalized in a visualization tool with many manual repeatable steps.
- Data is pulled from the source system for majority of metrics (e.g., Splunk, Qualys).
- Metrics are aligned to leading industry frameworks (e.g., NIST*, ISO*).

Managed

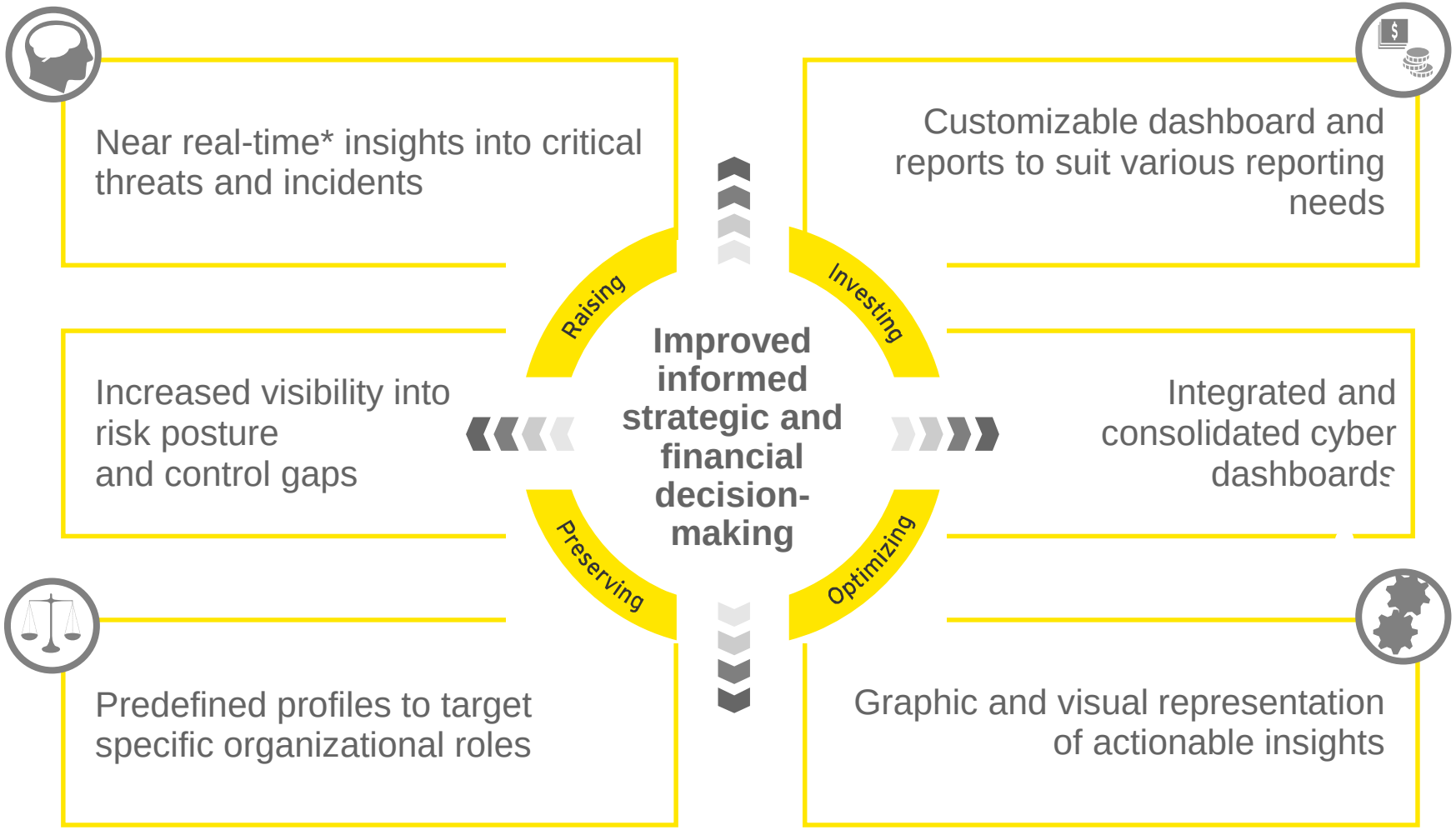
- Strategic and tactical metrics, KPIs* and KRIs* to monitor coverage and effectiveness.
- Dashboards leveraged for decision-making.
- Mostly automated dashboard; very limited manual effort.
- Most metrics pulled from source system in near real-time.
- Metrics measure health against industry frameworks.
- Dashboard audience expands to key executives (e.g., Board, Audit Committee).

Optimizing

- Dashboards are actively used in decision making.
- Real-time dashboard with advanced analytics capabilities driven by threat intelligence and predictive modeling.
- Granular views and broader audience (e.g., business units, Human Resources, Privacy, regional views, financial views).
- Dashboard utilized for communications and awareness across enterprise.

Fig. Maturity model for cybersecurity reporting

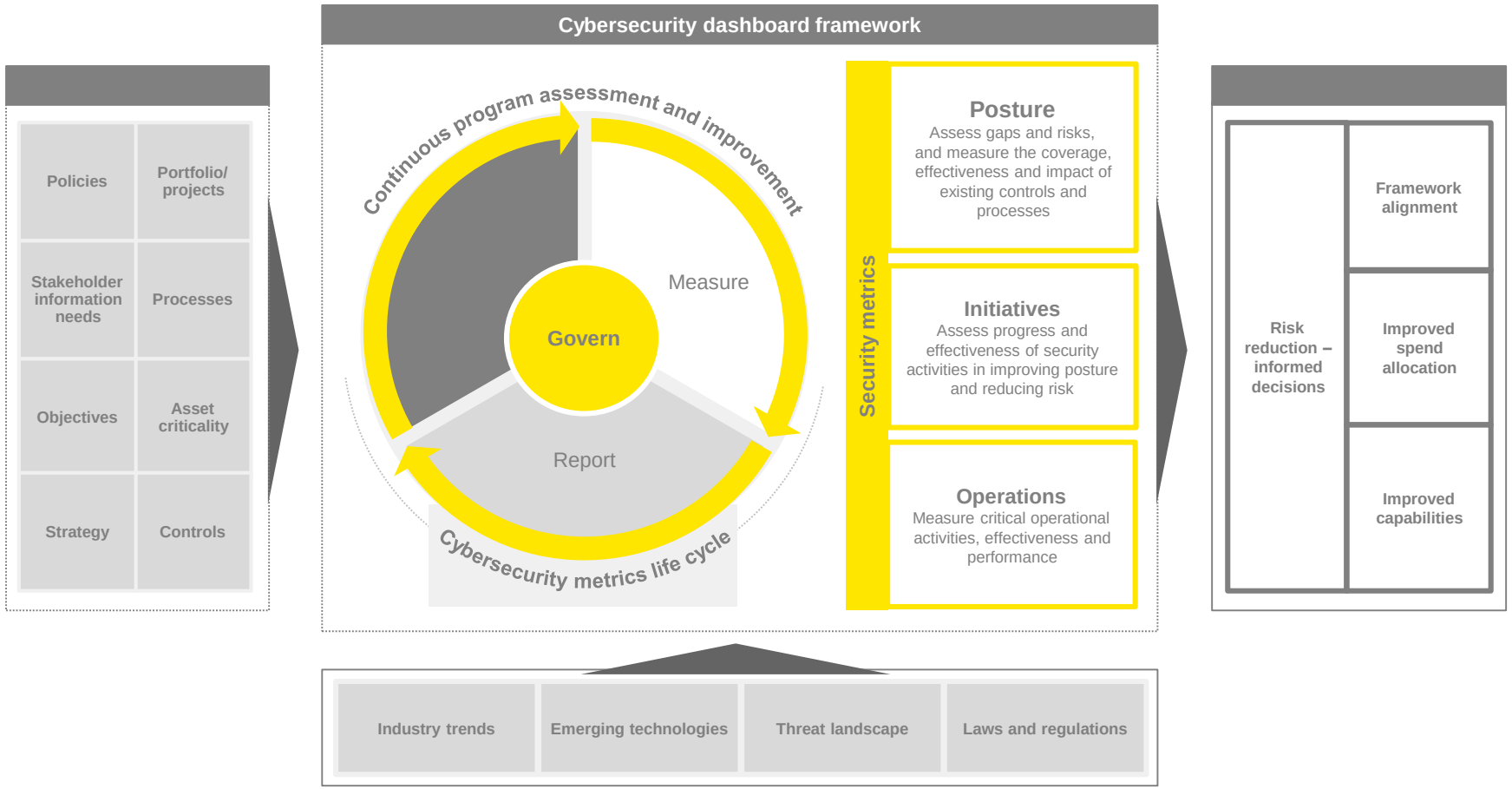
Cybersecurity dashboards can help provide tangible contributions to the organization.



*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.



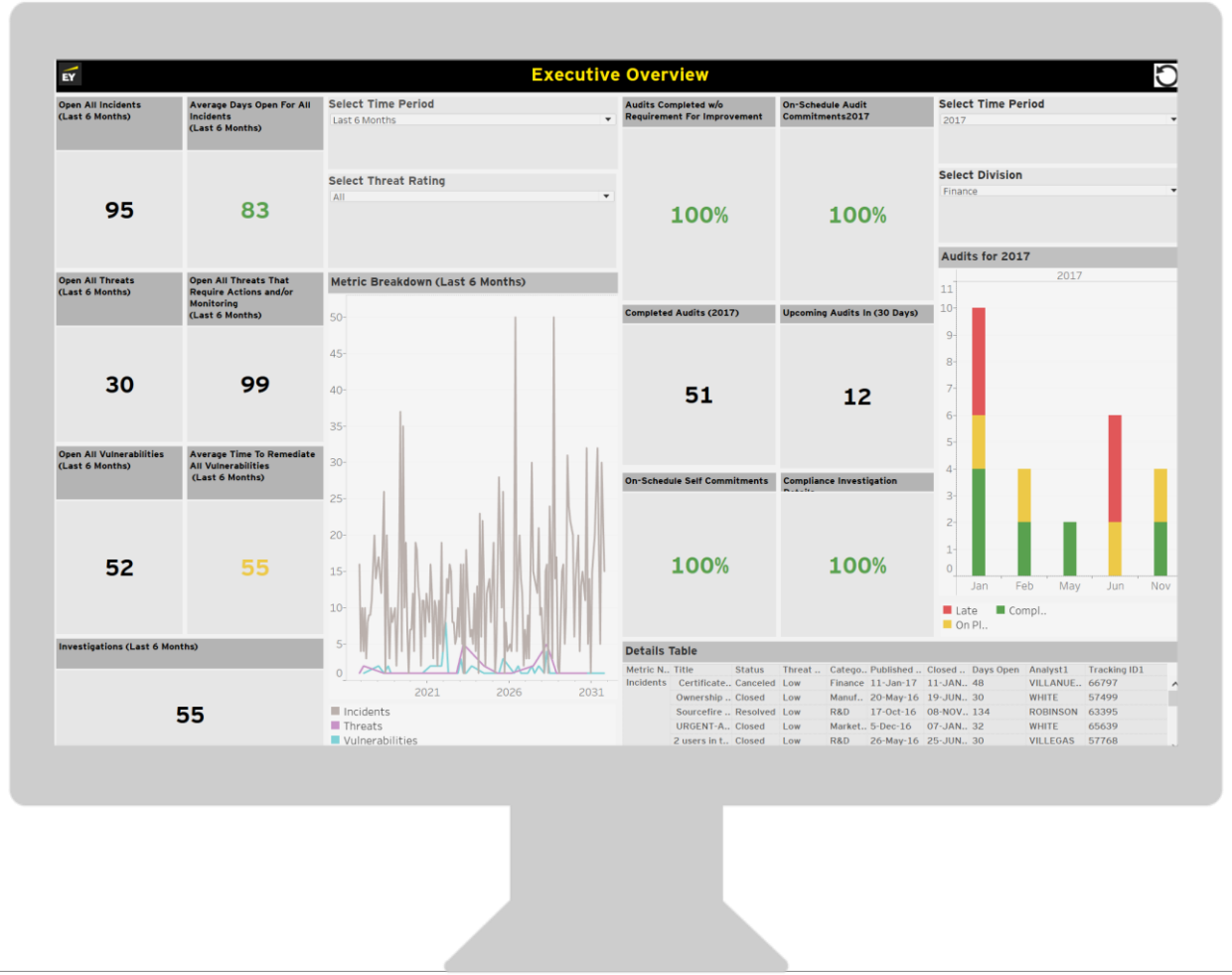
Sample dashboard artifacts

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

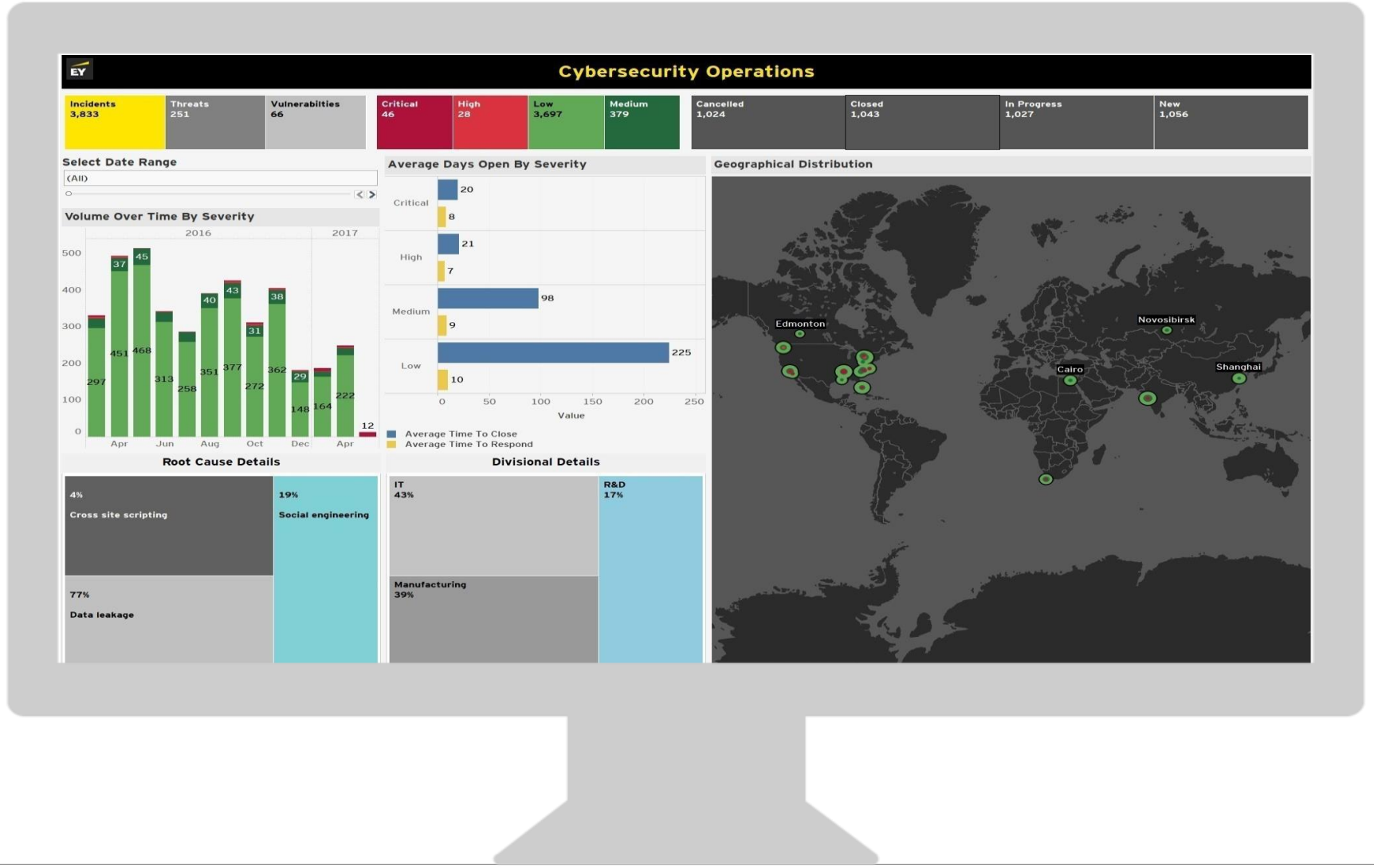


Demo dashboard: business unit overview

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

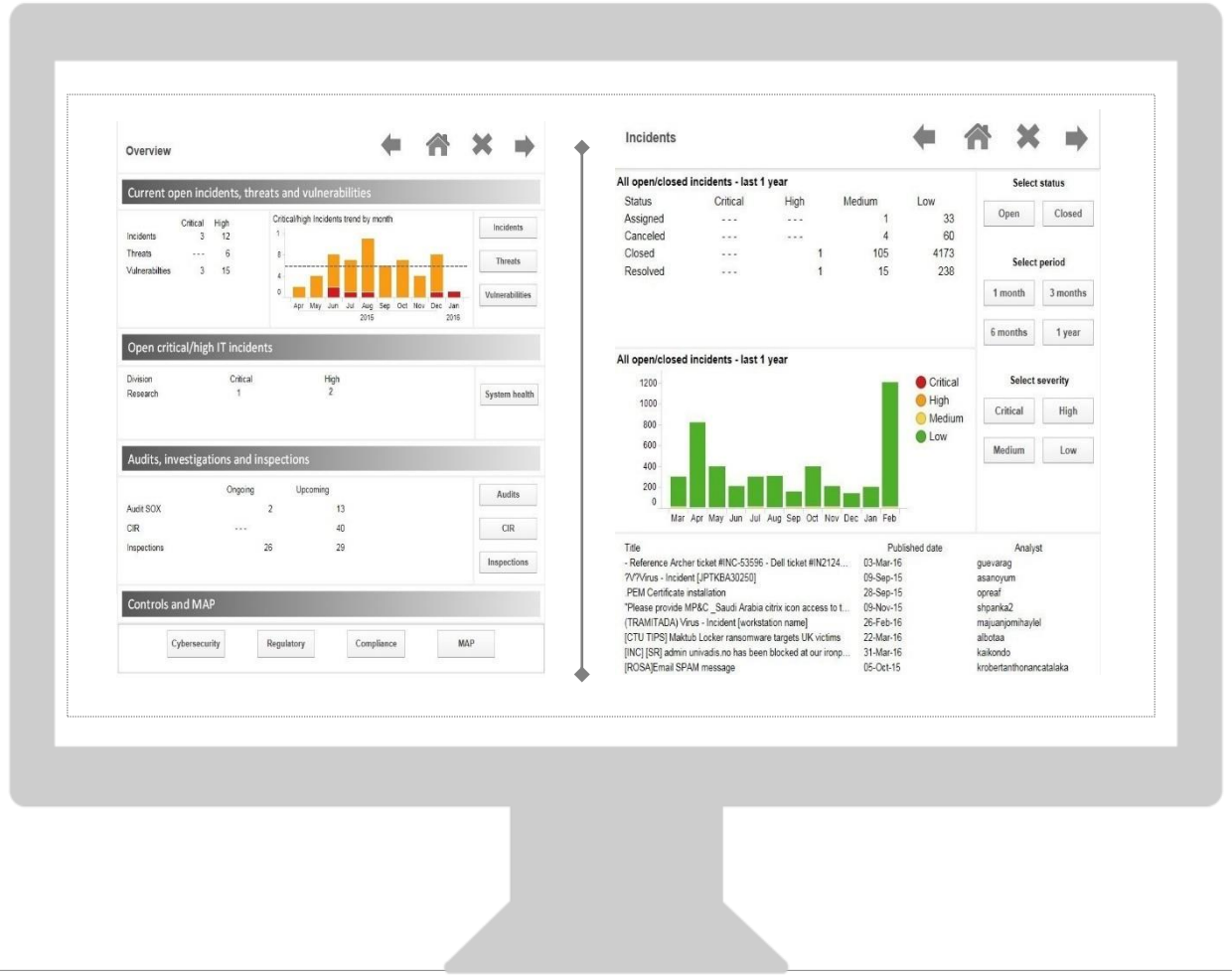
Demo dashboard: cyber operations

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



Lets Discuss……

EY | Assurance | Tax | Transactions | Advisory

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.

EYG no: 01799-183GBL

ED None

ey.com