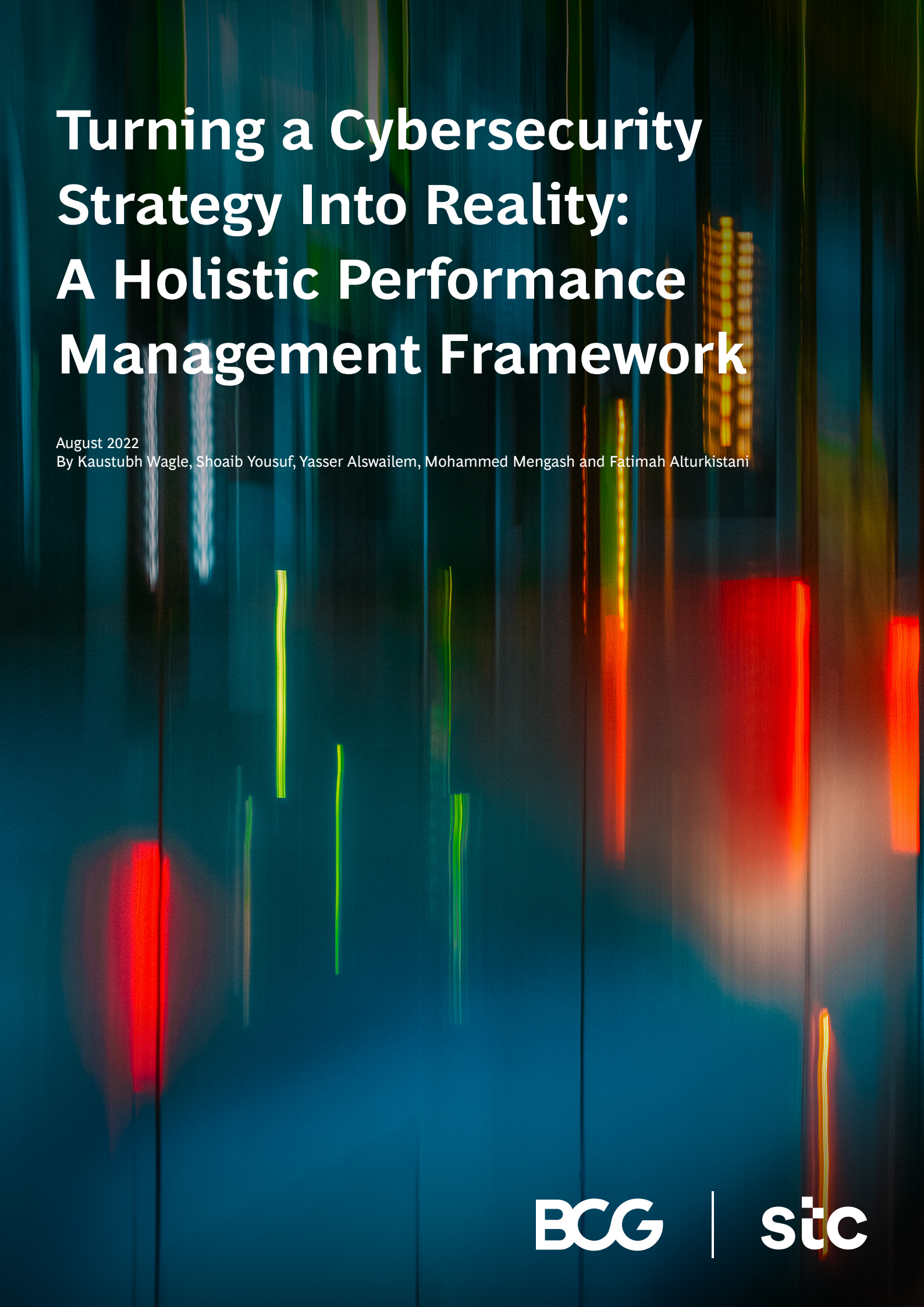


Turning a Cybersecurity Strategy Into Reality: A Holistic Performance Management Framework

August 2022

By Kaustubh Wagle, Shoaib Yousuf, Yasser Alswailem, Mohammed Mengash and Fatimah Alturkistani

BCG | stc

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

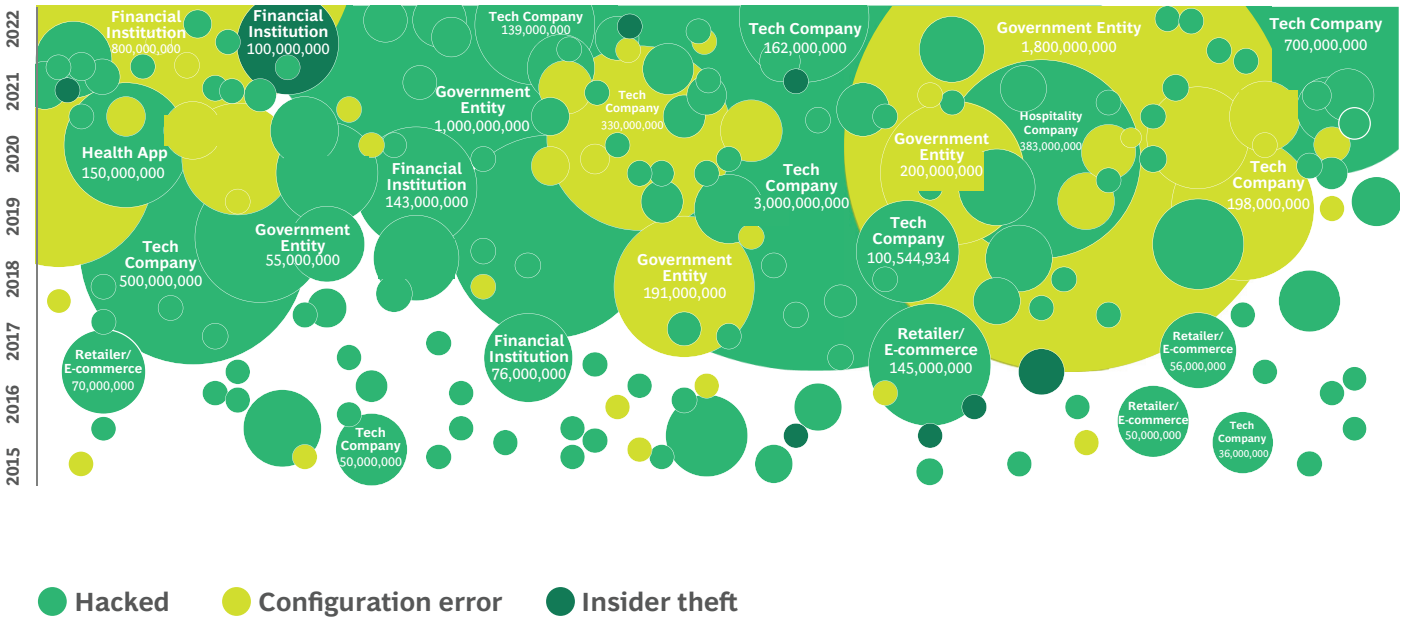
Saudi Telecommunication Company (stc) is the Saudi digital enabler of telecommunications services in the Kingdom of Saudi Arabia. stc are a pioneer digital champion, always been focused on innovation and evolution, thinking about the future to make it, to stay ahead as a truly meaningful and purposeful organization. stc offer variety of ICT solutions and digital services in several categories including telecommunication, IT, financial technology, digital media, cybersecurity, and other advanced digital solutions, with that stc are leading the digital transformation nationally and regionally.

Cyberattacks and breaches are not going anywhere.

The frequency and cost of cyberattacks is accelerating. Globally, the cost of cybercrime is estimated to have risen from $445B in 2015 to over $2.2 trillion today[1]. The frequency and size of data breaches are growing exponentially across all industries (Exhibit 1). In 2021, leading organizations across almost every sector reported major attacks, including tech companies, automotive[2] and government entities[3].

EXHIBIT 1

Massive Data Breaches Continued Unabated Throughout 2021



Source: FDataLossDB.org, informationisbeautiful.net, BCG analysis

Note: vs are of records reported stolen in a selection of publicly acknowledged breaches.

1. McAfee, CNBC, cybersecurity Ventures, and BCG Analysis
2. https://www.theregister.com/2021/05/21/toyota_cyber_attacks/
3. https://blog.sonicwall.com/en-us/2022/03/cyberattacks-on-government-skyrocketed-in-2021/

Meanwhile, advances in AI and the internet of things (IoT), combined with organizations' pandemic-accelerated adoption of flexible work arrangements and widespread digitization, have exponentially increased both our reliance on cybersecurity (CS) and the potential for attacks. The transition to 5G introduces another whole range of dangerous software-related vulnerabilities. According to the Brookings Institute, "never have the essential networks and services that define our lives, our economy, and our national security had so many participants, each reliant on the other—and none of which have the final responsibility for cybersecurity."[4] Looking forward, quantum computing – which may become widespread in as little as 5-10 years – will render today's encryption standards obsolete, with additional major implications for cybersecurity.

Cybersecurity has emerged as a critical risk management priority for public and private sector organizations alike. Spending on information security and risk management technology has increased dramatically and is estimated to reach $168B by the end of 2022[5]. The competition for scarce talent is fierce; an estimated 3.5 million cybersecurity jobs worldwide will go unfilled this year[6]. In this context, CEOs, Boards of Directors, and shareholders are anxious to understand the effectiveness and value of their cybersecurity investment and its overall contribution to the business. A recent Gartner article listed the following "five security questions your Board will definitely ask", as well as their underlying rationale and how a security leader might respond:

1. Incident
How did this happen? I thought you had this under control? What went wrong?

2. Tradeoff
It sounds like we are 100% secure? Are you sure?

3. Landscape
How bad is it out there? What about what happened at X company? How are we doing compared to others?

4. Risk
Do we know what our risks are? What keeps you up at night?

5. Performance
Are we appropriately allocating resources? Are we spending enough? Why are we spending so much?[7]

Faced with such questions, CISOs must be able to evaluate and report on their cybersecurity program's maturity based on top-level risks and outcomes and demonstrate to Board members how their organization is performing against its industry and peers. Discussing risks with senior executives has also proven to be a challenge, absent a common language that can be understood by both technical and non-technical stakeholders. The problem for CISOs is that these stakeholders generally lack the technical knowledge needed to understand the details of cybersecurity initiatives, even at the Board level. Highly technical security metrics must be summarized into accurate, easily understood, business-relevant insights for management, Board, and shareholders' meetings. This is where cybersecurity performance management can help.

Cybersecurity performance management is a process for evaluating the maturity of your cybersecurity program, systematically linking multiple levels of risk, metrics, investment and returns. When part of a coherent, ongoing process, these data-driven, dynamic measurements are valuable indicators of an organization's cybersecurity posture. Establishing a cybersecurity performance management program helps to baseline and prioritize what is important to the business, ensuring alignment with organizational goals and risk appetite, improving visibility, and achieving better outcomes from your security investment. Measuring cybersecurity performance across a range of relevant metrics allows organizations to target improvements, reducing vulnerability through corrective action.

Cybersecurity performance management enables CIOs and CISOs to answer the earlier questions, as well as:

- How are we performing against our adopted cybersecurity control framework(s)?
- What is our current maturity level?
- Are we making adequate investments? If not, where do investments need to be increased and why?
- What is our ideal future run-rate investment on cybersecurity?
- How much risk will we have once our run-rate is achieved?

Starting in 2019, Saudi Telecom Company (stc) partnered with Boston Consulting Group (BCG) to introduce a robust cybersecurity performance management framework as part of a larger cybersecurity transformation program. Its purpose was to track program execution progress and impact while providing a complete picture of stc's cybersecurity maturity. The framework has been implemented, reviewed, and improved over the past three years and has allowed stc to successfully realize its cybersecurity strategy. In this paper, stc and BCG would like to share the experience and lessons learned throughout this journey.

4. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cyber security/
5. Source: Gartner
6. https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cyber security-force.html
7. https://www.gartner.com/smarterwithgartner/5-security-questions-board-will-definitely-ask

1. Performance Management Framework.

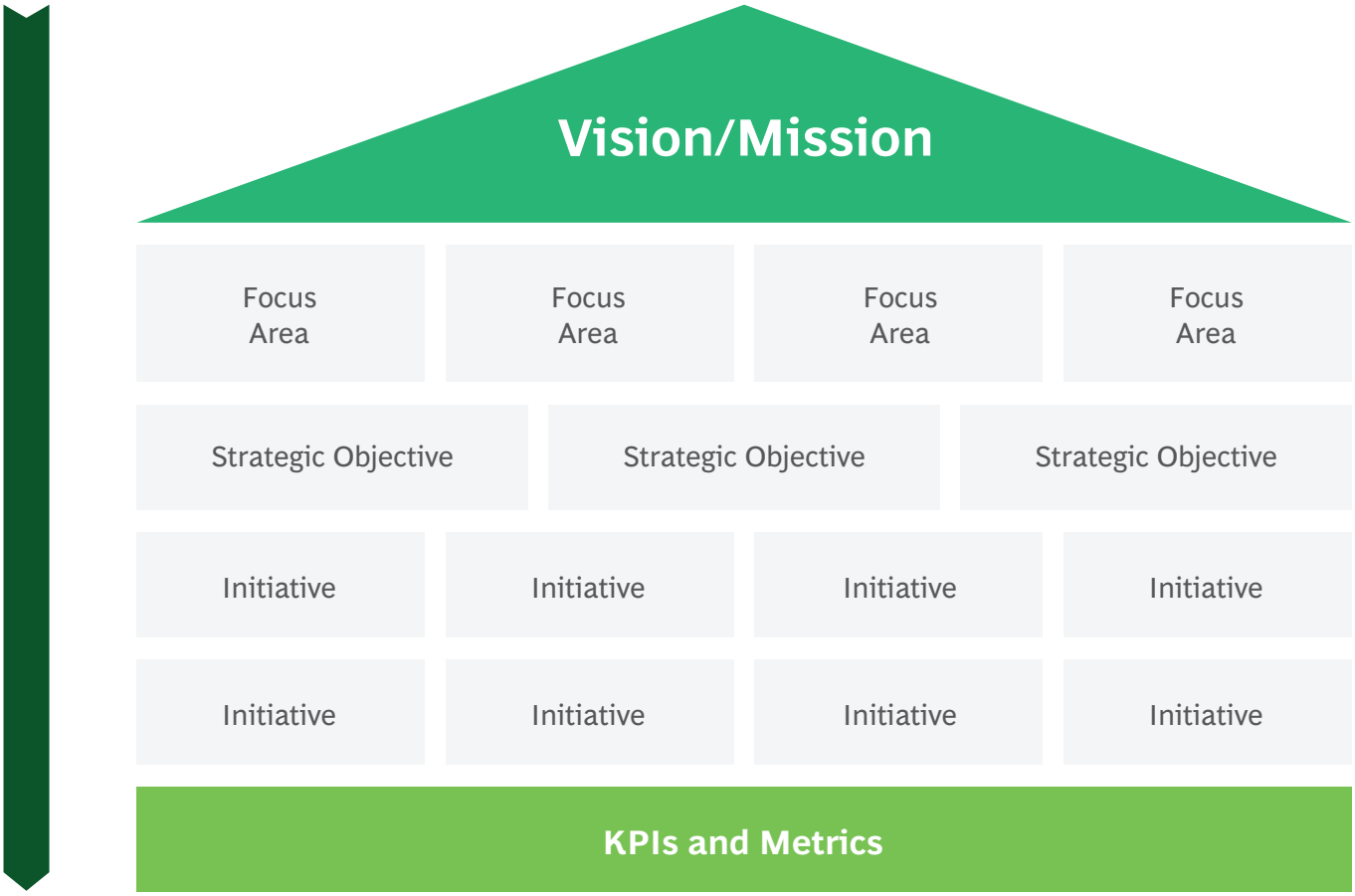
1.1 Shape the Cybersecurity Practice and Set the Direction

An effective performance management framework is derived from the cybersecurity strategy, that is driven in turn by the vision and mission of the CS program. Cybersecurity vision and mission play critical role in communicating the purpose of cybersecurity to stakeholders, developing a CS strategy, and measuring its performance and success.

Aligning the cybersecurity direction with business strategy is extremely important to reflect the internal and external context, mitigate risks and enable the business. A robust performance management framework is defined from the top down (Exhibit 2). Key Performance Indicators (KPIs) and metrics are derived from initiatives to achieve strategic objectives related to focus areas and CS capabilities (e.g., risk, governance, compliance, defense) that shape the cybersecurity practice and ensure business alignment.

EXHIBIT 2

Top- Down Approach for Performance Management



1.2 Quantify Cybersecurity Posture and Maturity

While most organizations are aware of cyber-risks, cybersecurity program maturity is uneven. It is vitally important for organizations to have an accurate understanding of where they are and how best to improve. Robust cybersecurity performance starts with a well-defined framework that enables organizations to elevate and benchmark performance across a wide range of CS capabilities, including strategy, business alignment, operating models, governance, risk, compliance, defense, etc. In 2019, with support from BCG, stc established a detailed Cybersecurity Framework. The framework identifies 30 initiatives to shape the cybersecurity practices and set the direction, enforce strategy, build CS capabilities, and secure the business. It reflects international standards and best practices from NIST, ISO 27001, and Gartner. Along with the framework, a tailored Maturity Model was established and defined (Exhibit 3), showing maturity levels for each cybersecurity capability. The model is used in health check assessments to determine the baseline, as well as progressive annual targets for cybersecurity maturity.

Cybersecurity Performance Management is the practice of measuring the organization's maturity in an objective and holistic way. These metrics allow cybersecurity leaders to assess performance of their current posture, while prioritizing security efforts, tracking progress, and reporting improvements over time. A holistic approach to performance measurement helps CISOs to systemically recognize and manage the reality that only 23% of breaches are caused by inadequate security technology, while the remaining 77% are due to failures related to organization, processes, or people[8].

Security strategy must strike an appropriate balance between investment in security capabilities and risk to the enterprise. Performance management helps identify gaps in strategy early, enabling informed, data-backed decisions about investment priorities and effective resource allocation. It also gives your security team the ability to benchmark your organization's security posture against similar organizations, placing cybersecurity in the larger business context.

EXHIBIT 3

Levels of Cybersecurity Maturity

Source: BCG

8. Source: BCG analysis of 50 major data breaches (2021) Source: BCG analysis of 50 major data breaches (2021)

Cybersecurity performance measurement and management should enable CISOs to automatically generate dynamic, visual dashboards for use by the Board, executive team, and security operations. In addition to providing a picture of current risks and performance, thoughtfully constructed dashboards link to longer term strategic and maturity goals, highlighting gaps and investment requirement, and accountabilities.

1.3 Define Cybersecurity Performance Management and Metrics

stc adopted a cybersecurity strategy and developed its performance management framework with assistance from BCG, as part of a larger effort to transform and advance the maturity of its cybersecurity capabilities. The performance management framework measures success via three sets of metrics, each focused on a different aspect of performance. From most granular to most strategic:

1. **Execution Index** tracks implementation of strategy initiatives. It answers the question: are we on track?

2. **Maturity Index** measures advances in security capabilities. It answers the question: are we improving?

3. **Transformational KPIs** monitor the impact of delivering on our strategic objectives toward a more robust security organization. They answer the question: are we realizing business impact?

Each *Performance Metric* is composed of connected sets of KPIs. KPIs are the critical indicators of progress toward an intended result. They provide a focus for strategic and operational improvement, create an analytical basis for decision making, and help keep attention on what matters most. As Peter Drucker famously said, "what gets measured gets done."

Within the performance management framework, each cybersecurity strategy initiative is translated into maturity KPIs, which are then aggregated into a *Maturity Index* for the cybersecurity program across initiatives. Maturity level per initiative is calculated by aggregating the individual maturity levels of its KPIs. For example, 'Security Architecture' is an initiative that may include maturity KPIs around the network architecture, application architecture and endpoint architecture. Another example is 'Endpoint Protection', which might translate into KPIs related to an endpoint protection suite, DLP solution, and Cyber Defense Center (CDC) integration.

All KPIs are based on measurements. They may be either ***qualitative*** or ***quantitative***, with qualitative metrics reported as words in levels, statements, and letters and quantitative ones reported as numbers, including proportions and ratios (Exhibit 3). For instance, 'Development and Maintenance of Frameworks' is a qualitative KPI, so measured in terms of maturity levels: L1 Frameworks not developed, L2 Frameworks developed, L3 Frameworks include high-level processes, L4 Frameworks include relevant stakeholders and L5 Frameworks have been reviewed in past 12 months. Qualitative metric owners need to supply proof of completion to ensure objective measurement, such as framework reviewed in past 12 months, alignment validated, or changes implemented and documented. Time from incident occurrence to detection, is a quantitative KPI, measured by the average timespan of the occurrence until detection of security incidents.

EXHIBIT 4

Qualitative vs. Quantitative Metrics Example

	Qualitative metrics are measured with levels	Quantitative metrics measured as percent or amount
METRIC	Development and Maintenance of Frameworks	Time from incident occurrence to detection
FORMULA	Maturity defined along following levels: • L1: Frameworks not developed • L2: Frameworks developed • L3: Frameworks include high-level processes • L4: Frameworks include relevant stakeholders • L5: Frameworks have been reviewed in past 12 months	Average timespan of occurrence until detection of security incidents
	"L3"	**"2 HOURS"**

2. Implementing the New Approach.

As with so many transformation programs, implementation was key to the success of stc's cybersecurity strategy. In this section we share what worked for stc – some decisions that paid off and lessons learned along the way.

2.1 Executive Support is Essential

Executive support is the most important key success factor. Effective cybersecurity performance management hinges on executives' willingness to prioritize, reinforce, and engage in an ongoing way with cybersecurity improvement efforts. It's not just technology that must change, but people's behavior throughout the organization – and that requires leadership commitment. Executives can demonstrate their support in several ways, for example:

- Participating in the development of KPIs that connect business vision and strategy with cybersecurity performance.
- Educating themselves and the Board so they can ask better questions and make business decisions that align with cybersecurity objectives.
- Investing the resources needed to meet cybersecurity maturity targets.
- Encouraging business owners to engage and align around their cybersecurity KPIs and targets.

2.2 Start with your Cybersecurity Strategy

Strategy is the starting point to achieving real business value from a cybersecurity program. Cybersecurity strategy includes vision, mission, strategic objectives, strategic initiatives, KPIs, and metrics. Its alignment with the corporate strategy and investment plan is crucial; cybersecurity is a key business enabler as organizations become increasingly heavy consumers of technology and data. Look for KPIs that link cybersecurity strategy to corporate strategic objectives.

Make sure that your cybersecurity strategy is not a just a static document, but includes a defined process for execution and outcome tracking. Especially since it is linked to performance management, this is an ongoing effort. stc found a key to success was keeping progress on track and removing obstacles in timely manner – so building that process into the strategy development will avoid delays later.

2.3 Choose and Define the Right Kpis

Developing key performance indicators can be tricky. KPIs need to be well defined and weighted according to critical or core business objectives. Exhibit 4 illustrates stc's approach to defining KPIs. The headline is not enough. stc created a card for each KPI summarizing its name, ID, initiative affiliation, owner, measurement frequency, data source, description and rationale, measurement formula, performance level, target, and index weighting. As well making CS and business stakeholders think through the details of each KPI, the cards increase the reliability of tracking and provide important consistency across diverse KPIs.

- **KPI name:** reflects what this KPI is meant to measure in easy-to-understand language
- **KPI ID:** unique identity code to be used in the KPI catalogue
- **Initiative** name of the initiative that is linked to this KPI
- **Owner:** person responsible for providing KPI metrics to the Performance Management Team along with evidence
- **Measurement frequency:** reporting cycle for the KPI – may be monthly, quarterly, or annually
- **Data source:** agreed tool or method to provide evidence for the reported KPI metric – subsequently validated by the Performance Management Team
- **Rationale and description:** explain the KPI itself and why it is important
- **Formula:** how to calculate the KPI value
- **Performance level:** scale to define different maturity levels, to be assessed against the set target
- **Targets:** expected maturity level to be achieved – typically increasing over time
- **Weight:** if you have a KPI that have a sub-KPIs, weighting is assigned across sub-KPIs proportionally according to importance and contribution

EXHIBIT 5

Sample KPI Card: Development and Maintenance of Frameworks

Initiative	Owner	Measurement freq.	Data source
G1: CS Frameworks	**Governance**	**Yearly**	**Framework change logs**

DESCRIPTION AND RATIONALE

Governance is the legislative body of cybersecurity and as such develops

FORMULA

Maturity defined along following levels:

- L1: Frameworks not developed
- L2: Frameworks developed
- L3: Frameworks include high-level processes
- L4: Frameworks include relevant stakeholders
- L5: Frameworks have been reviewed in past 12 months

MATURITY LEVELS

TARGETS

2019	2020	2021	2022
4	5	5	5

WEIGHT

5

Out of 5

2.4 Ensure a Clear Process for KPI Collection and Validation

stc established a formal Performance Management Team responsible for identifying KPIs, collecting reports, and validating data. KPI reports are collected based on their defined cycle (monthly, quarterly, yearly) or upon a specific request from management. The KPI owners provide current values to the Performance Management Team including relevant evidence to ensure transparency on how the values were derived and corroborate the provided values. This clear accountability – KPI owners, Performance Management Team – is key to an effective ongoing program.

The Performance Team then validates the values. If the provided evidence does not correspond with submitted values, they request the KPI owner to resubmit. There are two general validation levels for each KPI:

- **Level 1: Accuracy of data source.**
  Making sure that the submitted evidence is from the data source identified in the KPI definition.
- **Level 2: Consistency of the data.**
  Making sure that evidence supports and is consistent with the value assigned. For example, if the qualitative metric says, "frameworks have been reviewed in past 12 months", then the documentation log should show the changes during past 12 months.

After validating the data, the Performance Management Team aggregates all collected values into dashboard to report to management.

2.5 Use Trend Analysis to Track Cybersecurity Performance Over Time vs. Maturity Targets

Once the validation stage is complete and submitted values for the cycle are accepted, analysis begins, comparing actual KPI values with their targets. This is essentially the step that takes us from performance ***measurement*** to performance ***management***. Trend analysis reports should capture any major deviations from the KPI's cybersecurity maturity target, or from cybersecurity strategy execution initiatives. Results are then provided to top management who can evaluate these trends against cybersecurity targets and strategic objectives.

3. Cybersecurity Metrics Monitoring, Review and Continuous Improvements.

3.1 Periodic Reports and Committee Meetings

Cybersecurity KPI measurements, and the maturity levels to which they aggregate, are important inputs for CISO decision making. But they must also be shared beyond the cybersecurity department and incorporated into leadership's balanced scorecard reviews. This should happen at least quarterly or, more commonly, monthly based on an organization's needs. Especially when an organization is trying to track the effects of an important change, or in other situations where rapid feedback is needed, reports should be generated and shared monthly. They enable business leaders to monitor performance issues and provide timely support.

stc uses two main cybersecurity performance reports:

1. **High Level Report of Cybersecurity Performance Metrics.** Selected indicators, including the overall maturity level score along with the maturity scores for each strategic initiative. This gives top management the "big picture" of cybersecurity performance.

2. **Detailed Report of Cybersecurity Performance Metrics.** Used in conjunction with the high-level report, this more detailed report includes maturity level scores and analysis for each KPI, broken out by initiative and department. This report is typically used by top cybersecurity management, in discussion with KPI owners.

A cybersecurity Performance Management Committee (PMC) is responsible for monitoring performance and guiding the execution of Cyber Operations and Strategy. Using the detailed cybersecurity performance metrics report as its main source of reference, this committee meets on monthly basis to:

- Review each department KPIs (Strategy and Function Unit KPIs)
- Validate KPIs and confirm that they remain fit for purpose
- Monitor strategic initiatives' execution status and target milestones
- Highlight and address cross-functional dependencies and challenges
- Provide support as needed
- Realign, refresh, and improve sector strategic direction and operational excellence
- Monitor strategy execution risks and ensure proper mitigation steps are considered
- Improve strategic and operational execution, updating projects, tasks, processes, and procedures as needed
- Approve any KPI change requests

3.2 Cybersecurity KPI Change Management

Maturity indices are used to measure the organization's overall security posture. Following the principle of "you get what you measure", it is important to choose the right metrics and adjust them if necessary. Especially in the first year of operation, or when conditions are changing rapidly, the approach must be flexible enough to accommodate learning from experience. It is not necessary to wait until the end of an improvement cycle. KPIs may be adjusted during the year if needed, for example if:

- Cybersecurity mandates or structure have changed
- New regulations have been released
- New capabilities are needed
- The existing KPI or its definition is not yielding the necessary information

To adjust a KPI, stc requires a Change Request (CR) to be completed by its owner, including justification for the change. After the KPI owner's manager approves the request, it goes to the cybersecurity Performance Management Team for review and feedback. Finally, after the KPI owner and Performance Management Team are aligned, the CR needs to be approved by the PMC.

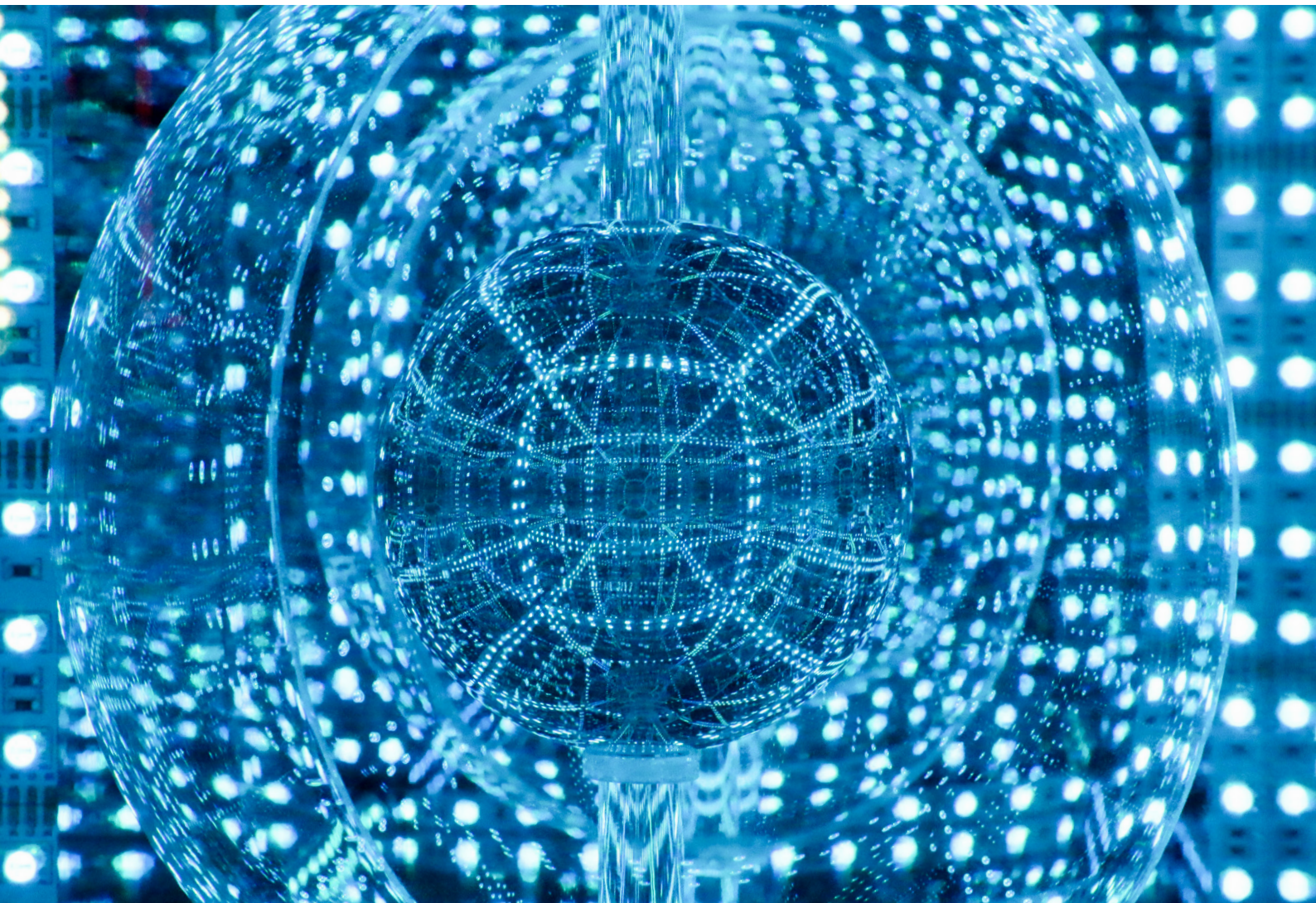
In addition to ad hoc changes of the kind noted above, an organization should build periodic metrics review and improvement into its cybersecurity performance management process. Such a review might cover each KPI's rationale, formula, targets, and reporting cycle.

Realizing the Benefits.

Companies around the world are redoubling their focus on cybersecurity as a business-critical capability. Increasingly, they are recognizing the need for holistic approaches, integrated with their business strategy and goals. Since introducing their cybersecurity strategy and performance management program, stc has seen a host of benefits including:

- An end-to-end cybersecurity strategy that builds capabilities, strengthens foundational controls, implements advanced controls, and sharpens monitoring.
- Robust cybersecurity performance management that plays a significant role in elevating cybersecurity maturity, improving accountability and task ownership.
- Elevated cybersecurity maturity and strategy alignment across group subsidiaries. (stc extended support and guidance to subsidiaries to implement cybersecurity strategy, and measure their cybersecurity capabilities through customized performance packages for each subsidiary.)

With dramatic increases in cyberattacks' pace, frequency and cost, companies are seeking to learn from each other, identifying and adapting best practices to move faster and stay ahead of evolving threats. In response to this need, and in recognition that cybersecurity is an urgent global priority, stc and BCG are happy to share this paper.



About the Authors

Kaustubh Wagle is a Managing Director and Partner in BCG's Middle East office. He is a core member of BCG's Technology, Media & Telecommunications practice. You may contact him by email at Wagle.Kaustubh@bcg.com.

Shoaib Yousuf is a Managing Director & Partner in BCG's Middle East office. He is a core member of BCG's Technology, Media & Telecommunications practice. You may contact him by email at Yousuf.Shoaib@bcg.com.

Yasser Alswailem is the VP of Cyber Security at stc and a board member of Sirar by stc. You may contact him by email at yalswailem@stc.com.sa

Mohammed Almengash is the General Manager of Cybersecurity Strategy and Engineering at stc. You may contact him by email at mmengash@stc.com.sa.

Dr. Fatimah Alturkistani is the Cybersecurity Enablement Director at stc. You may contact her by email at falturkistani@stc.com.sa.

Acknowledgement

The authors are grateful to the broader team of BCG and stc colleagues, alumni, and industry peers whose insights and experiences contributed to this white paper. This BCG insight paper was prepared in collaboration with stc and namely, Arwa Alhamad, Basma Ahmadush and Wagieh Saad. If you would like to discuss this report, please contact the authors.


BCG
stc