Chapter 11
Organizational Intelligence: Cybersecurity as a Performance Optimizer

Rhonda Farrell

Recent cybersecurity innovations in both technology and standards, set a new tone for organizations, allowing for cyber-intelligence to be capitalized on by focusing on continuous collection, analysis, policy enforcement, and remediation at multiple enterprise levels. Vast improvements in governance, risk, and compliance management follow.

Focusing on these three areas allows for enhanced collaboration with strategy, change management, and quality efforts, allowing for heightened performance and personnel optimization.

Organizational Intelligence

What if the operating model were changed to use cybersecurity-related capabilities as the model for organizational performance optimization efforts?

Is it possible that leaders could drastically transform enterprise practices, by better enabling cyber initiatives to lead the way by focusing on integrating capabilities, tools, and data?

Would organizations be willing to enhance their governance, risk, and compliance efforts by incorporating model elements from the cyber realm?

More importantly will cyber leaders and executives be willing to step out of their comfort zone and examine the rapidly changing worlds of strategy, change management, and organizational excellence for ideas, practices, and quantitative method-

R. Farrell (✉)

D.A. Christofferson (ed.), *Women in Security*, Women in Engineering and Science, https://doi.org/10.1007/978-3-319-57795-1_11

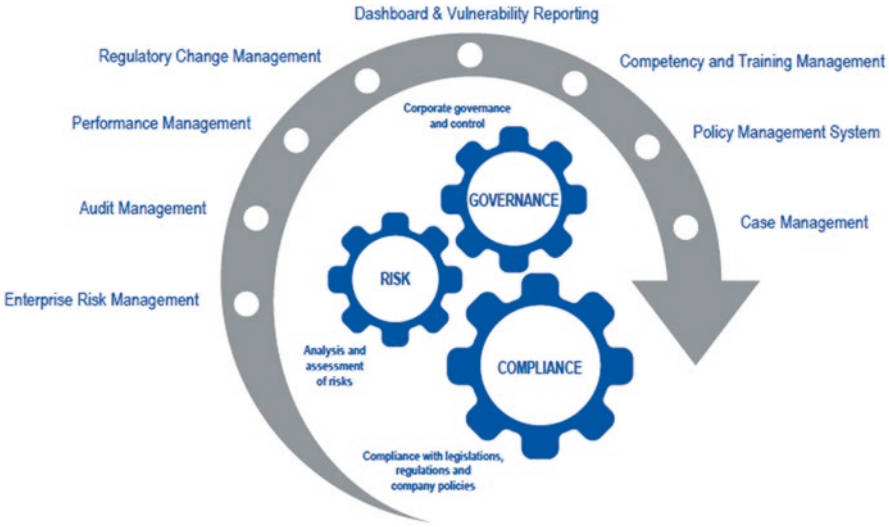

Fig. 11.1 Typical GRC suite of services (http://www.360factors.com/information-security-risk-management-software/vulnerability-risk-management/)

ologies that will raise the bar significantly in the areas of engagement, ethics, value, and sustainability?

Figure 11.1, below shows a typical Governance, Risk, and Compliance (GRC) services suite which focuses heavily on standard organizational elements which allow for organizations to identity, manage, and remediate risks across the enterprise.

The components listed below offer a solid baseline to work from and offer plenty of maturation opportunities, as the focus turns to WHY, HOW, and to WHAT EFFECT initiative implementation will have on the organization, products, services, stakeholders, and most importantly, the workforce.

Getting leaders and practitioners to focus on the WHY behind the action tends to be the game changer—as this allows for the core components relating to the organization's people, process, and technologies to be identified. Once these basic elements have been thought through and enumerated, further strategic alignment activities can occur to mission, vision, goals, objectives, and key performance indicators.

Taking a methodical examination of the enterprise interconnect points, oftentimes paves the way for enablement of the widest possible re-use to maximize value across the entire organization.

These initial discovery, planning, and strategy undertakings often leads to the publishing of initial outputs, allowing for the larger stakeholder base to emulate the "WHY" exercise at the local levels, thereby unlocking innovation and performance opportunities and enhancing organizational business intelligence capabilities, per Fig. 11.2.

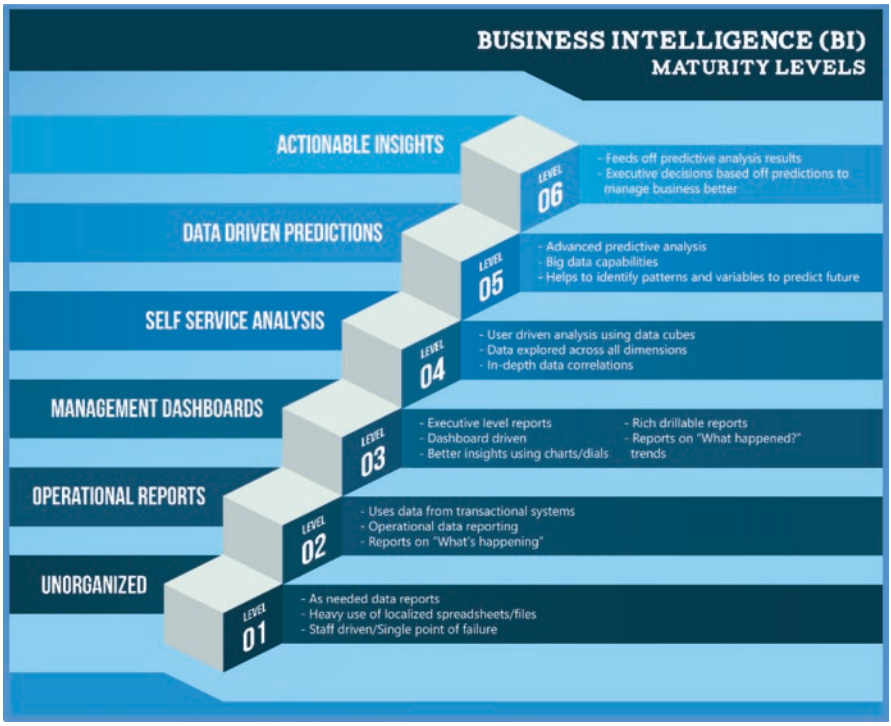

Fig. 11.2 Business intelligence maturity model (http://www.ventera.com/news/insight/white-paper-sensible-approach-successful-business-intelligence-biimplementation)

The focus on maturing cybersecurity related GRC initiatives oftentimes provides for rich data deposits that can be mined for product, service, infrastructure, and business capability creation purposes. Additionally, it also helps identify workforce densities and geographic disbursement patterns, thus opening the door to further knowledge management, collaboration, and information sharing efficiencies.

Examining cyber generated data through the business intelligence lens and continually asking how the data and information can inform, focuses not only on hardening the WHY, but also addresses the HOW behind making the initial operating leap to using a constantly questioning, analyzing, and innovating, data driven approach.

As Fig. 11.2 shows, incorporating a business intelligence model informed by cyber generated information can lead to a much wider perspective on value creation across the enterprise. One of the results could be a more robust GRC services suite, augmented to include these new capabilities, much like Fig. 11.3 below.

Primarily the reader will notice that with the addition of the business intelligence element, the product and service capabilities can then also drive towards answering the TO WHAT EFFECT inquiry that must be done to drive further efficiency and effectiveness gains (see Transformation related activities).

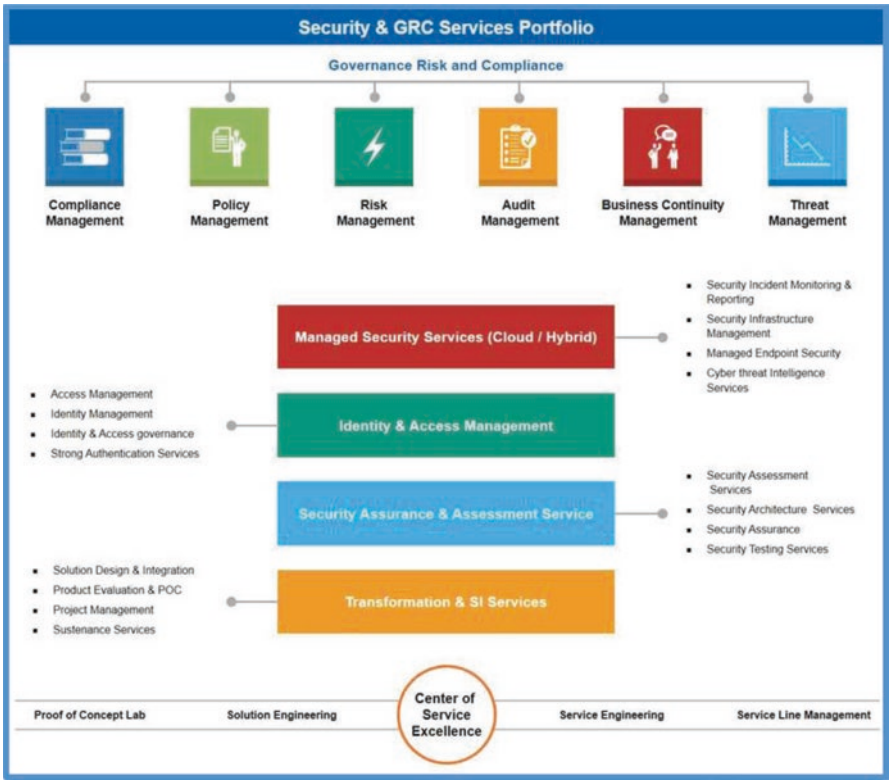

Fig. 11.3 Enhanced GRC suite (https://www.hcltech.com/it-infrastructure-management/information-security-services)

Even though the rudimentary basics of WHY, WHAT, and TO WHAT EFFECT are being consistently addressed by using quantitative analysis on risks, compliance assessments, and corporate governance findings, several key programmatic components may still be lacking or immature, disallowing or impacting organizational leaders in their quest to take their programs to the next level.

Foremost among these highly optimizing program elements are performance management, solid leadership practices, workforce engagement, utilization of enhanced knowledge management systems, and most important, high involvement customer/client management.

Figure 11.4 outlines the core process components as extracted from the Baldrige Excellence Framework (2015–2016). For those non-familiars, this body of knowledge focuses on a "systems approach to improving your organization's performance" as well as undertaking actions which "empower your organization to reach its goals, improve results, and become more competitive" (pp. title, i).

Fig. 11.4 Baldrige—organizational excellence—key process perspective (http://www.baldrige21.com/Baldrige%20Model.html)

Not only does this body of knowledge help enterprises solidify their WHY, it offers a flexible methodology for ascertaining a set of HOWs approach, as well as incorporates a heavy Performance Management focus, which helps organizations harden their TO WHAT EFFECT inquiry and projections.

In addition to expounding upon the core Baldrige processes as outlined in Fig. 11.4, the National Institute of Standards and Technology (NIST) recently released the Baldrige Cybersecurity Excellence Builder, which informs key cybersecurity leadersVhip and practitioners on key organizational excellence elements they can put in place to harden their overall cybersecurity programs, while at the same time strengthening the bonds between the realms of cybersecurity and quality overall.

Figure 11.5 depicts the organization cyber-related roles associated with expected use of this new guidance, as well as benefit enumeration which can be achieved organizationally, thus bolstering the case of the addition of heightened business intelligence capabilities to inform enterprise decision-making on a wider scale.

Once the core Baldrige building blocks have been put into place the harder work of ensuring strategic alignment within the organization must then be used to tear down silos of inefficiency and pave the way for transparent communication and collaboration efforts.

Who in an organization should use the *Baldrige Cybersecurity Excellence Builder*?

The *Baldrige Cybersecurity Excellence Builder* is intended for use by the leaders and managers in your organization who are concerned with and responsible for mission-driven, cybersecurity-related policy and operations. These leaders and managers may include senior leaders, chief security officers, and chief information officers, among others.

Role/Function	Benefit of/Reason for Using the *Baldrige Cybersecurity Excellence Builder*
Board and Executive Management	• Understand how internal and external cybersecurity should support organizational (business) objectives, including support for customers • Understand current and planned workforce engagement processes and their success • Understand opportunities to improve cybersecurity in alignment with organizational objectives • Understand the potential exposure of the organization's assets to various risks • Align cybersecurity policy and practices with the organization's mission, vision, and values
Chief Information Officer (CIO)	• Understand how cybersecurity affects organizational information management practices and culture • Improve communication and engagement with organizational leaders and the cybersecurity workforce • Understand how cybersecurity affects the organization's culture and environment
Chief Information Security Officer (CISO)	• Support the organization's commitment to legal and ethical behavior • Create and apply cybersecurity policy and practices to support the organization's mission, vision, and values • Respond to rapid or unexpected organizational or external changes • Support continuous improvement through periodic use of the self-assessment tool • Support organizational understanding of compliance with various contractual and/or regulatory requirements • Understand the effectiveness of workforce communication, learning, and engagement, as well as operational considerations for cybersecurity.
IT Process Management	• Improve understanding of business requirements and mission objectives and their priorities • Determine the effectiveness of IT processes and potential improvements • Understand how aspects of cybersecurity are integrated with organizational change management processes
Risk Management	• Discern the impact of cybersecurity on internal/external customers, partners, and workforce • Improve understanding of how workforce engagement in cybersecurity and communication to the workforce about cybersecurity impact the organization's overall risk posture
Legal/Compliance Roles	• Understand legal/ethical behavior on the part of the workforce, as well as the overall cultural environment • Understand how the organization applies cybersecurity-related policies and operations to ensure responsible governance, including legal, regulatory, and community concerns
Employees (Workforce)	• Understand leaders' expectations • Be better prepared for changes in cybersecurity capability and capacity needs • Benefit from a workplace culture and environment characterized by open communication, high performance, and engagement in cybersecurity matters • Learn to fulfill their cybersecurity roles and responsibilities

Fig. 11.5 Baldrige—organizational excellence—key process perspective (https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf)

Often-times these initiatives focus on enhancing the mission and vision of the organization, enterprise, or business unit. It may also entail defining new goals and objectives which focus on heightened mission achievement, flowing from the enhanced strategy, which in turn inform new or updated policies.

Innovation and technology capabilities are then oftentimes acquired or developed to provide enhanced analytics surrounding programmatic and technical risk to quantify likelihood or impact with increasing rigor. Additionally, cyber hardening initiatives oftentimes focus on enhancing:

(a) workforce capabilities to meet mission need;

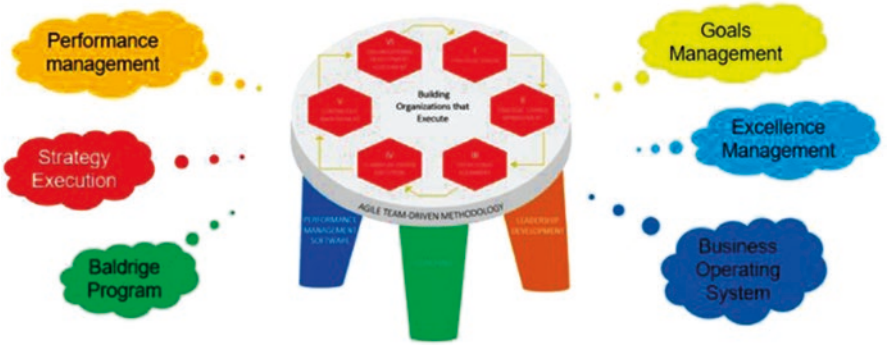

Fig. 11.6 Organizational excellence building blocks for Agile organizations (https://www.linkedin.com/pulse/organizational-excellence-building-agile-organization-gary-harpst)

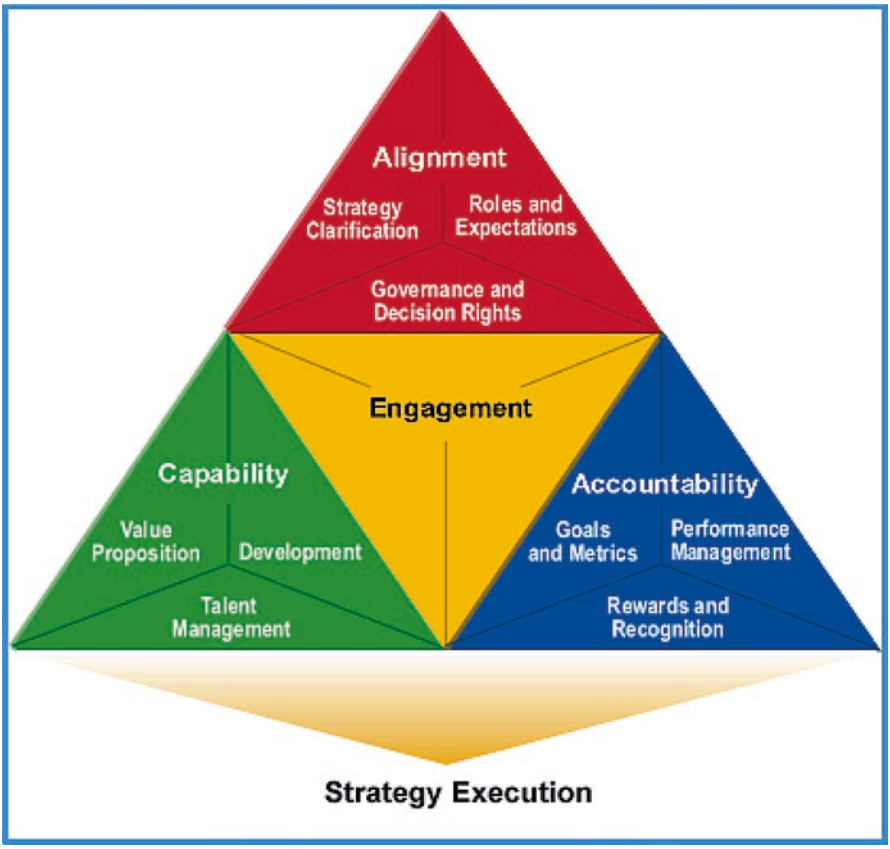

Fig. 11.7 Strategy execution (http://www.sibson.com/services/organization-talent/strategy-execution/)

(b) wide-spread and in-depth process improvement; or
(c) business process re-engineering to better capitalize on the plethora of findings generated by the business intelligence algorithms. Figure 11.6 outlines the organizational excellence elements necessary to enable programmatic success.

Figure 11.7 shows an example of a more robust strategy execution model, depicting the strong ties between heightened governance practices, high levels of workforce and leadership engagement, value-laden capability development, paired with stringent performance management practices, and generous rewards and recognition when high levels of mission achievement are the ultimate result.

Once the core Baldrige components have been steeped from both an organizational optimization and cybersecurity perspective longer term continuous improvement program elements can then be put into place. This entails examining the organization holistically, at a far deeper level, focusing on triaging trouble-spots, innovating through difficulties, and providing enriched value-add capabilities, both externally, as well as internally.

Figure 11.8 depicts the enhanced and broadened organizational capabilities which are achievable once a solid baseline of Baldrige, enhanced business intelligence capabilities, and more resilient cybersecurity practices are put into place. Note the added focus on culture, trust, core values, and value enhancing activities on multiple levels.

Following the iterative, efficiencies, effectiveness, and productivity gains achievable via implementation of the methodologies, practices, and components listed

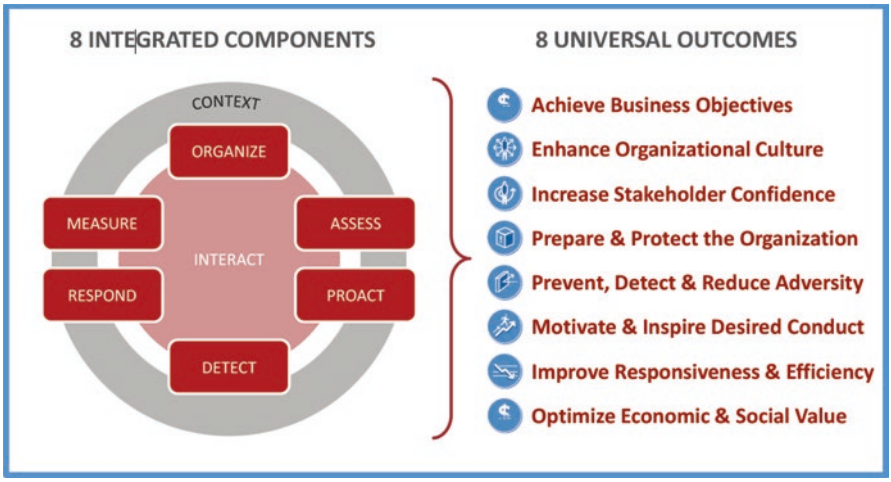

Fig. 11.8 Organizational intelligence (http://www.oceg.org/resources/grc-capability-model-red-book-2/)

Fig. 11.9 The key model elements (http://www.bendelta.com/news/strategy/effective-leadership-important-for-strategy-execution/)

above, Fig. 11.9 shows the highly recognizable key elements associated with driving continual success for your organization.

Never fear, as once the enterprise has achieved this interim plateau called 'success', where everything makes sense, at least for some modicum amount of time, it's almost certain that industry will innovate beyond, requiring the organization (and you) to rethink your WHY once again.

Never doubt the process, for as the organization keeps shooting for the moon, they'll reach the STARS a million times over, raising morale, building momentum, and creating sustainable motivation to continue to the next level of maturity and performance optimization.

Here's to much Baldrige inspired success for you and your organization!