Cybersecurity Management Program

whitepaper

Cybersecurity Managment Program

Many organization's cybersecurity teams (or information security teams as they used to be known) continue to struggle to communicate cybersecurity issues to senior leadership. Likewise, senior management also struggles to effectively articulate cybersecurity strategy to technical cybersecurity personnel. It is as though two parts of the same organization speak foreign languages to one another, and each party has a very limited, or no, knowledge of the other party's language. However, it does not have to be like this.

Failure to communicate issues is most often revealed in grassroots cybersecurity initiatives that have evolved into corporate cybersecurity programs. Typically, this resulted from an enterprise in startup mode implementing solutions to address specific technical challenges. Unfortunately, many organizations continue to employ a similar approach to secure much larger and more complex environments against threats that outmatch the capabilities of their original solutions. No longer simply a technical solution, cybersecurity management has become a business function in today's industry. As a business function, a greater level of integration with other business units requires a greater level of transparency and performance reporting.

The evolution of grassroots cybersecurity programs rarely results in the kind of mature cybersecurity solutions that are aligned with, and address business needs. And why should they? The initial programs were designed to solve technical challenges, such as preventing virus outbreak or infection, stopping cyber attackers from compromising or stealing valuable information. Such initial cybersecurity efforts were neither designed as business functions nor defined in business terms.

Key Success Factors

The following key success factors are common to many successful cybersecurity programs. The programs:

- Support and drive strong governance attitudes and actions
- Are designed, developed, and implemented in a similar way to other business functions
- Adopt a standard framework approach, usable for an extended period of many years with little or no changes to that framework
- Are measureable in terms of their effectiveness

Organizations and executives that drive successful cybersecurity programs do so in the same manner as other successful business initiatives. Executives succeed at this not because of industry pressure, but because each aims to improve their organization. Having identified the opportunity, executives evaluate whether the initiative poses additional risks to their organizations and decide whether to accept this additional risk or not. After accepting such risk, executive sponsors continue to evaluate initiatives toward implementation. Even when initiatives are operational, executives still employ strong governance methods, including internal audit teams, to manage and monitor the effectiveness and efficiency of these initiatives. This business approach has become institutionalized across most enterprise units with the exception of IT and cybersecurity. Key stakeholders in IT and cybersecurity often claim that cybersecurity management programs are too technical, only internal facing, or too complex, to properly develop and implement using this approach.

The truth is if these same IT and cybersecurity groups adopted a common framework and designed their cybersecurity management programs based on said framework, cybersecurity management would truly become just a standard business function in their enterprises. Unfortunately, the cybersecurity world does not agree on a standard cybersecurity framework across all countries, industries, and states. Analysis of the commonalities and differences between these standard frameworks show that it is possible to create a universal cybersecurity management framework to address all countries, industries, and states. Such a framework is not firmly associated with any particular cybersecurity standard and can be adapted during implementation to address any specific security standard that organizations using it wishes to follow. This paper introduces a cybersecurity management framework where it is apparent that a successful approach is not too technical, addresses both internal and external concerns, and is not overly complex to implement, operationalize, and manage over the long term.

Cybersecurity Management Framework

The design of the Cisco cybersecurity management framework (CMF) assumes cybersecurity management is a business function.

Analysis of the commonalities and differences between these standard frameworks show that it is possible to create a universal cybersecurity management framework to address all countries, industries, and states.

The framework, as a business function, is comprised of three discrete pillars with each subsequent layer unfolding increasing levels of specificity as follows:

The **Executive Management (Strategy) Pillar** directs Governance and Planning initiatives that drive the framework forward to operation.

- The Executive Management Pillar requires people to identify why cybersecurity is needed, consider the business issues, and then define, document, and publish the direction the required cybersecurity program will adopt.

The **Operations Pillar** that defines what the cybersecurity program must address to comply with the requirements specified in the strategy, what supporting functions are needed, and what level of reporting/governance monitoring should be provided. These needs are supported through the security intelligence, IT and Cybersecurity Assurance and IT Risk Management operations sub-pillars.

- The Operations Pillar requires definitions of documented operational standards, processes, procedures, and other collateral that specify what operators should do and how they should do it.

The **Tactical (Technology) Pillar** defines how required cybersecurity controls mandated in the Operations and Executive Management pillars will be applied to the systems, networks and applications used by the organization and how evidence will be provided to management that the security controls implemented actually address the specific requirements and that they perform their job as expected.

- The security controls in the Tactical pillar, whether requiring technology or not, are responsible for securing all aspects of an enterprise computing environment, continuously monitoring the environment for security events, collecting and analyzing captured events, and reporting defined security metrics, some of which are provided to the SLT.

Although addressing cybersecurity challenges with just three pillars is perfectly possible, adopting and using it in that way is difficult and potentially open to error or misinterpretation. To minimize these issues, these macro-level pillars must be divided into more manageable chunks. The Cisco CMF subdivides its three macro pillars into seven discrete focus areas:

- **Executive Management**: Key decisions and accountability required to drive the program
- **IT Risk Management**: Reducing risk exposure to the organization to a level acceptable to the SLT and Board of Directors.
- **Cybersecurity Intelligence**: Required to provide the cybersecurity and IT teams with appropriate information to achieve and surpass IT Risk Management goals.
- **IT and Cybersecurity Assurance**: Required to provide evidence to management and especially the SLT that their investments in cybersecurity are delivering the benefits they expected.
- **Secure Network**: Required to support secure, on demand access to information to authorized personnel no matter where it is located within, or external to, the organization.
- **Secure Systems**: Required to provide controlled access to applications, data and devices according to the identity of the requesting party. This focus area also includes how data is protected, whether at rest, or in transit.
- **Secure Applications**: Required to control access to data and other networks, systems and applications according to the identity of the requesting party. For internally developed applications, requirements extend to how the application was designed, developed and managed throughout the whole development lifecycle.

While these seven focus areas provide increasing granularity, the framework introduces an additional level of subdivision to ensure practitioners can readily apply and manage the CMF. In total, the CMF model is subdivided into 40 (forty) cybersecurity elements as shown in Figure 1 on page three.

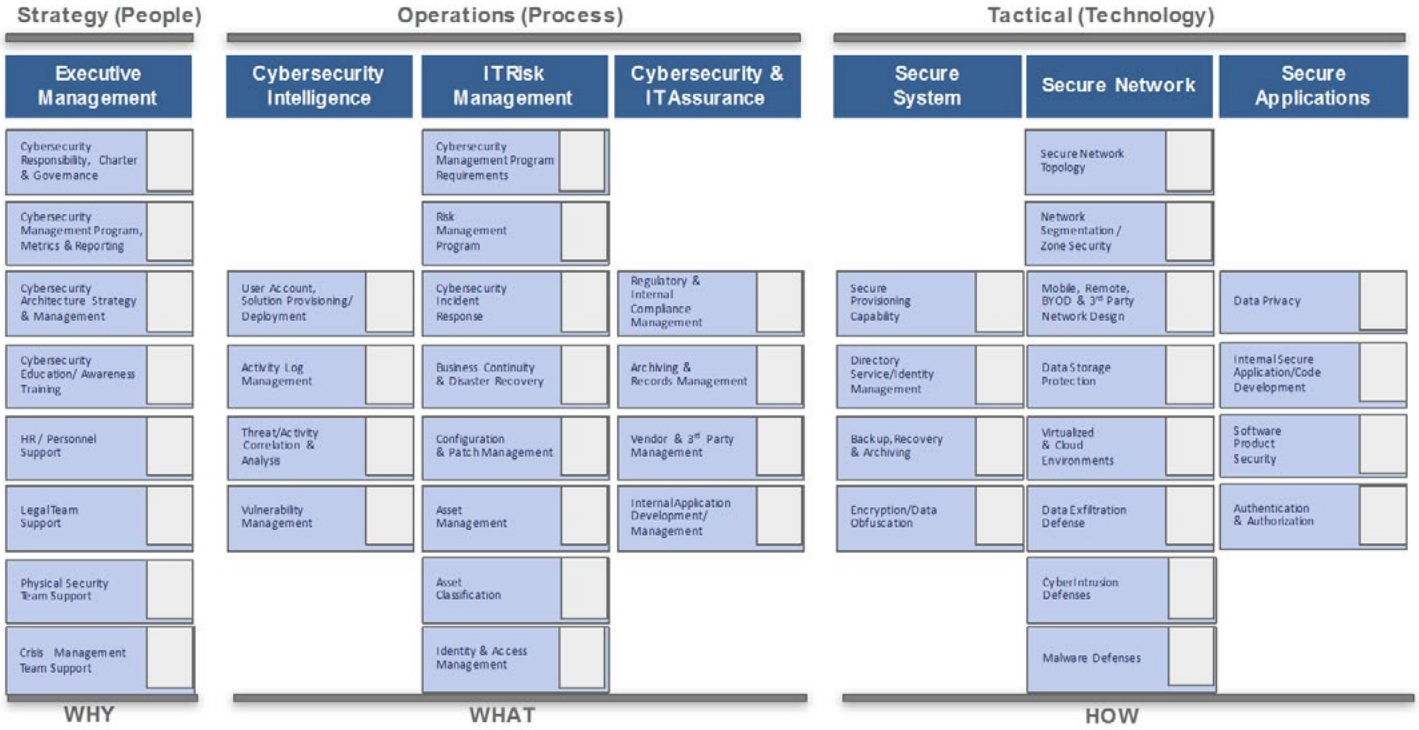

Figure 1: Cisco Cybersecurity Management Framework

Cybersecurity Management Framework Adoption and Usage

The Cisco CMF (figure 1) shows how an organization should consider its own program. In a perfect, green-field situation with little pressure to protect exposed assets, an organization may not experience any difficulty with implementing this framework. Unfortunately, few organizations fit this reality and thus are not afforded the luxury of green-field framework adoption. Existing organizations must continue to generate revenue to stat in business.

It is possible to operate with an unstructured non-framework based approach, but as many have found out, there is a significant chance that areas of concern will be missed and that they will be 'cracks' in the security barriers erected that do permit compromises to occur, and possible remain undetected and unresolved for significant periods of time.

Preferred Choice

The Cisco CMF, or any similar framework, supports a holistic approach to cybersecurity, which most cybersecurity professionals recommend. An organization's existing program, no matter its current state, can adopt a cybersecurity management framework to benefit from consistency of approach and integration inherent to framework. Though implementing such a framework may consume more time and resources, it is important to remember that achieving cybersecurity is not an endpoint, it's a journey. So, too, is transitioning a grassroots, tactically driven, approach to a business-focused cybersecurity program based on a formal cybersecurity management framework.

As with all journeys, an organization must define a starting point. This is the time at which executive management realizes cybersecurity is not simply an IT function but instead a business function employing controls (people, process, technology) to address specific security. Approaching security in this way guides leaders to understand the logical next step is defining a security strategy. Moreover, it becomes clear that such a security strategy is not defined by IT or the cybersecurity team, but a strategy defined by management. Such a business management strategy clearly articulates a risk based approach, one that all members of the SLT and the board of directors (or equivalent) easily and readily understand. It is a strategy, defined by people, that informs an organization that information is vital to the success of the organization and mandates that protecting such assets appropriately is not just a good idea, it is essential. Protecting the organizations' information assets is a responsibility everyone in the organization shares.

As the SLT defines the strategic way forward, stakeholders must evaluate and understand risks facing the organization associated with compromise, loss, or theft of information. The SLT has a responsibility to the organizations stakeholders to reduce risk to acceptable levels—or eliminate risk altogether. While it is possible for an organization to completely eliminate all risk, such an organization would effectively cease business operations because the cybersecurity protective controls applied would likely prevent access to information or make it very difficult to consume. "Perfect" cybersecurity effectively acts as a business disabler, not a business enabler.

To enable and support an organization's business objectives and goals, a cybersecurity program must allow authorized users access to information. This means organizational leadership must accept and manage risk concerning information compromise, loss, or theft. In short, the SLT must evaluate, understand, and accept some amount of risk when users access information assets. The question is, how much?

Accepting risk may not be a path an SLT is comfortable navigating. Typically, this is where an SLT might hand off the problem to a corporate risk-management committee, or team, who, together with the chief information officer (CIO) or chief information security officer (CISO), define and agree on an overarching cybersecurity policy and potentially a cybersecurity charter. These documents articulate the general need for a risk-based cybersecurity management program (CMP), who or which teams are responsible for its definition, and which individuals and/or teams have responsibility for supporting or taking actions according to a charter, or policy, mandate. The highest level of corporate leadership (chief executive officer (CEO) or board of directors) must approve and endorse these documents. Requirements specified in these documents should be business relevant and only change as business goals and objectives change. Organizations should always require a cybersecurity policy, but some CEOs prefer to endorse a cybersecurity charter that outlines the need for cybersecurity, but delegates responsibility and authority for definition of the policy that drives the CMP definition and operation.

Program strategy is the starting point from which an organization migrates its existing program to the new program based on a cybersecurity management framework. It doesn't matter what an organization's current level of sophistication is, or its complexity or maturity with regard to its security program. Any organization is able to commit to a business-focused cybersecurity program addressing SLT concerns as mandated, endorsed, and expressly articulated in the cybersecurity charter and policy. Together these elements support the governance necessary to effectively manage the Program.

Transforming an Existing Cybersecurity Program

As stated earlier, achieving a specific cybersecurity maturity level is a journey. When planning any journey, you cannot proceed without identifying a starting point and an endpoint. Given these parameters, you then determine a timeline between these two points and categorize constraining variables, if any, that can impact the journey. Security policy, to a large degree, defines the endpoint to the journey and protects the organization's information assets. The Policy should only contain 'evergreen' statements that will not require changes due to timelines, budgets, or other business variables as the approved and endorsed Policy content should remain static and require few, if any, changes. Each of these is a risk that stakeholders must consider when developing their organization's cybersecurity program.

Initially, IT and cybersecurity teams own responsibility for reviewing existing cybersecurity standards and processes. They are responsible for determination of whether documented requirements meet the spirit of the policy or need to be modified to do so. Following that, the stakeholders (IT, cybersecurity, and often business unit owners of data and applications) meet with the risk committee, and/or steering committee, to consider whether adoption of the proposed standards and procedures will present unacceptable risk to the organization's information assets or users. To provide maximum ROI, stakeholders prioritize process and procedure documentation (not accounted for during the assessment) during this time. Additionally, stakeholders introduce supporting technologies, or updated tactical configurations, that are needed to address specific cybersecurity concerns.

Some organizations may try to achieve a best-in-class level of cybersecurity by implementing the framework through a single-step transition (from their current level of cybersecurity maturity). In all likelihood, this approach will fail unless organizations have, for the most part, already achieved their desired maturity levels. Without such preexisting programs in place, transitions are typically too burdensome and likely will result in a cybersecurity program that does not satisfy SLT-defined requirements. Prudent organizations should properly assess their cybersecurity program's current status or maturity, and subsequently use assessment results to define a baseline position from which the organization is capable of executing incremental improvements over 2 to 5 years to reach an acceptable cybersecurity maturity level that is similar to, or slightly ahead of, their peer organizations.

It is worth noting that any desire to reach optimal levels of cybersecurity concerning each element within the framework has the propensity to consume significant resources, can result in exceedingly rising costs, and, as such, result in an unsatisfactory ROI. Setting and achieving lower but risk-acceptable levels of cybersecurity maturity across the framework will result in compliance with requirements in a much shorter timeframe, provide enhanced ROI, and strongly limit the window of opportunity during which successful cyber attacks can occur.

Cybersecurity Maturity

Any cybersecurity transformation process, such as the one this paper describes, requires an organization to measure and monitor improvement for a given cybersecurity element in terms of its maturity level. The authors of Cisco CMF adapted the Carnegie Mellon University (CMU) Capability Maturity Model (CMM) to better suit cybersecurity programs. CMU introduced its CMM to drive improvements in software development together with similar approaches documented by ISACA. In all cases, the term maturity refers to the degree of formality and optimization of processes from unplanned or initial practices to formally defined steps to managed results metrics to active optimization of the processes used during application and program development.

The Cisco CMF uses predefined maturity-level requirements for each security element to objectively assess the sophistication or maturity of the documented approach. Each maturity level assigned to each element is a numeric value. Focus area maturity values are a combination of maturity values for element associated with a given focus area. Program stakeholders can then combine focus-area maturity scores to provide an overall maturity score for the Cisco CMF layer and finally convey an overall cybersecurity program maturity level.

In practice, the authors of the Cisco CMF have experienced that most organizations using this approach usually ignore layer-level and total program-maturity scores and concentrate solely on the focus area and individual cybersecurity element maturity scores. This is most likely because responsibility for specific cybersecurity elements or focus areas is far easier and more effective to delegate and manage than it is for a layer of the model or indeed the whole model.

Although the CMU and ISACA CMM maturity descriptions consist of five levels, the authors here found it essential to add a sixth level applicable to the cybersecurity world. This was necessary because some countries, industries, and organizations do not include certain cybersecurity elements in their programs. Allocating such elements, those not considered or implemented by an organization, a zero value ensures that the mathematics behind the model remain consistent and are not skewed by false level 1 maturity scores.

At a high level, the maturity definitions defined with the Cisco CMF are summarized in Figure 2

Maturity Level		
Level 0 Absent	0	**Absent;** no identifiable or documented cybersecurity controls or practices
Level 1 Initial	1	**Initial;** acknowledgement that cybersecurity controls are necessary and improvements are in progress
Level 2 Repeatable	2	**Repeatable;** multiple controls and processes documented, some areas still managed via 'tribal knowledge'
Level 3 Defined	3	**Defined;** all controls documented and widely implemented, but not yet enterprise wide
Level 4 Managed	4	**Managed;** enterprise wide implementation, measurement metrics regularly reported. Regular controls review & updates
Level 5 Optimal	5	**Optimal;** Best-in-class control set, always seeking improvements, acknowledged as cybersecurity leader in the vertical industry

The Cisco CMF uses predefined maturity-level requirements for each security element to objectively assess the sophistication or maturity of the documented approach.

Every element in the Cisco CMF contains multiple sub-elements, each of which receives a set of maturity definitions. As such, the CMF has a maturity-level definition library consisting of several hundred entries. In addition to the number of unique entries, cybersecurity elements often possess multiple interdependencies between one another. These resulting relationships drive analysis of findings from a simple maturity assessment to one that takes into consideration these multidimensional aspects. This approach also applies to development of recommendations necessary to improve maturity of a given cybersecurity element.

Successful CMP Development: Ten Key Success Factors

Organizations should not underestimate the difficulty of developing and implementing a cybersecurity management program (CMP). The introduction of a CMP affects virtually every individual or group in an organization, so it is essential that the final cybersecurity program best address everyone's needs.

Ciso's experience in developing CMPs indicates that the following statements are 10 key success factors. If organizations apply these statements in the order given, it has the highest probability for successfully developing, implementing and managing a CMP:

1. Identify and gain support and commitment from a member of the SLT to introduce a CMP.

2. Develop an enterprise wide cybersecurity program charter (effectively the cybersecurity strategy for your organization) and submit to the CMP sponsor for socialization with the SLT and endorsement by the CEO.

3. Create a CMP project work plan, the first task of which is to develop the cybersecurity policy. In larger enterprises, it is likely that multiple PMs may be necessary.

4. Establish and mandate usage of a document review and version management system to support ongoing management of CMP documentation.

5. Complete work on the CMFs Strategic elements first. However, it is also likely that multiple elements may be developed in parallel especially where there are no or few dependencies between the elements.

6. Define elements so that each element contains at least one security metric definition and identifiable data source to support metrics generation.

7. Identify and treat as high-priority development efforts key elements with enterprise wide impact such as architecture related elements and core elements that are a foundation to many other elements.

8. Review all documented elements for consistency and accuracy prior to developing elemental dependencies associated with the element(s) under review/revision.

9. Develop all remaining elements having dependency on key elements followed by elements having no dependencies.

10. Dedicate time and effort to develop consistent, congruent and easily understood documentation that clearly describes the what, why, when, where, how, and who is responsible for every action required by the program.

You should notice that just applying these 10 key success factors to cybersecurity program efforts does not necessarily guarantee short-term success. It is more likely that following this framework and applying the 10 key success factors will enable a successful cybersecurity management program to emerge over the long term.

Summary

Development, implementation, and maintenance of a cybersecurity management program for an organization is no small undertaking. However, the overall value that organizations achieve through development and implementation of such programs includes reduced instances of successful cyber attacks. Moreover, a cybersecurity management program provides organizations with a means to reduce a successful attack's impact on the bottom line due to its programmatic predefined approach for identifying and responding to cybersecurity incidents.

Read more about cybersecurity management programs and Cisco Security Services at www.cisco.com/go/securityservices.