Cybersecurity Management Programs

White Paper

Dr. J. Stuart Broderick,
CISM, CRISC, CCSK
Principal
Cisco Security Solutions
June 2015

Most organizations' cybersecurity teams (or information security teams as they are sometimes known) 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 management 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 management 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

Many successful cybersecurity management programs share the following key success factors:

- 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 performance and efficiency

Examining each of these factors in detail, you may find that executives initiate successful cybersecurity management programs 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 internal audit teams to 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 often cite reasons, including programs are too technical, only internal-facing, or too complex, to properly evaluate or implement this same approach to cybersecurity.

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

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 a standard business function in their enterprises. Unfortunately, the cybersecurity world does not agree on a standard cybersecurity framework, much less across all countries, industries, and states. Analysis of the commonalities and differences between the various frameworks in use 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 wish to follow. This paper introduces a cybersecurity management framework that is not too technical, addresses both internal and external concerns, and is not overly complex to implement, operationalize, and manage over the long term.

Senior leadership teams (SLTs) provide greater support to, and are more confident of, the usefulness and effectiveness of their organizations' cybersecurity management programs if those programs provide regular, useful, and usable metrics. Unfortunately, many cybersecurity professionals inundate their SLT with large quantities of data presented in ways that sometimes require extended explanations. A more effective approach is to first determine specific metrics most beneficial to their SLTs followed by a reporting regime that addresses those specific concerns. Simplifying SLT cybersecurity reporting can be as uncomplicated as a single number or individual letter, a colored graphic or a few sparklines on a webpage, or something less likely to grow into a really detailed report.

The framework described in this paper was developed based on thousands of hours of working with organizations of all sizes and across all industries. This framework is designed to be used globally, across industry sectors, without change, and is applicable to organizations of any size.

Cybersecurity Management Framework

The design of the Cybersecurity Management Framework (CMF) assumes cybersecurity management is a business function. The framework, as a business function, requires three discrete layers with each subsequent layer unfolding increasing levels of specificity as follows:

- **Strategy** is to initiate and drive the framework forward to operation.
  - Requires people to identify the need for cybersecurity, consider the business issues, and then define, document, and publish the direction the required cybersecurity management program will adopt.
- **Operational** focus defines what the cybersecurity management program must address to comply with the requirements specified in the strategy.
  - Requires definitions of documented operational standards, processes, procedures, and other collateral that specify what operators should do and how they should do it.
- **Tactical** security controls address specific requirements articulated in the operational documentation.
  - These security controls, 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.

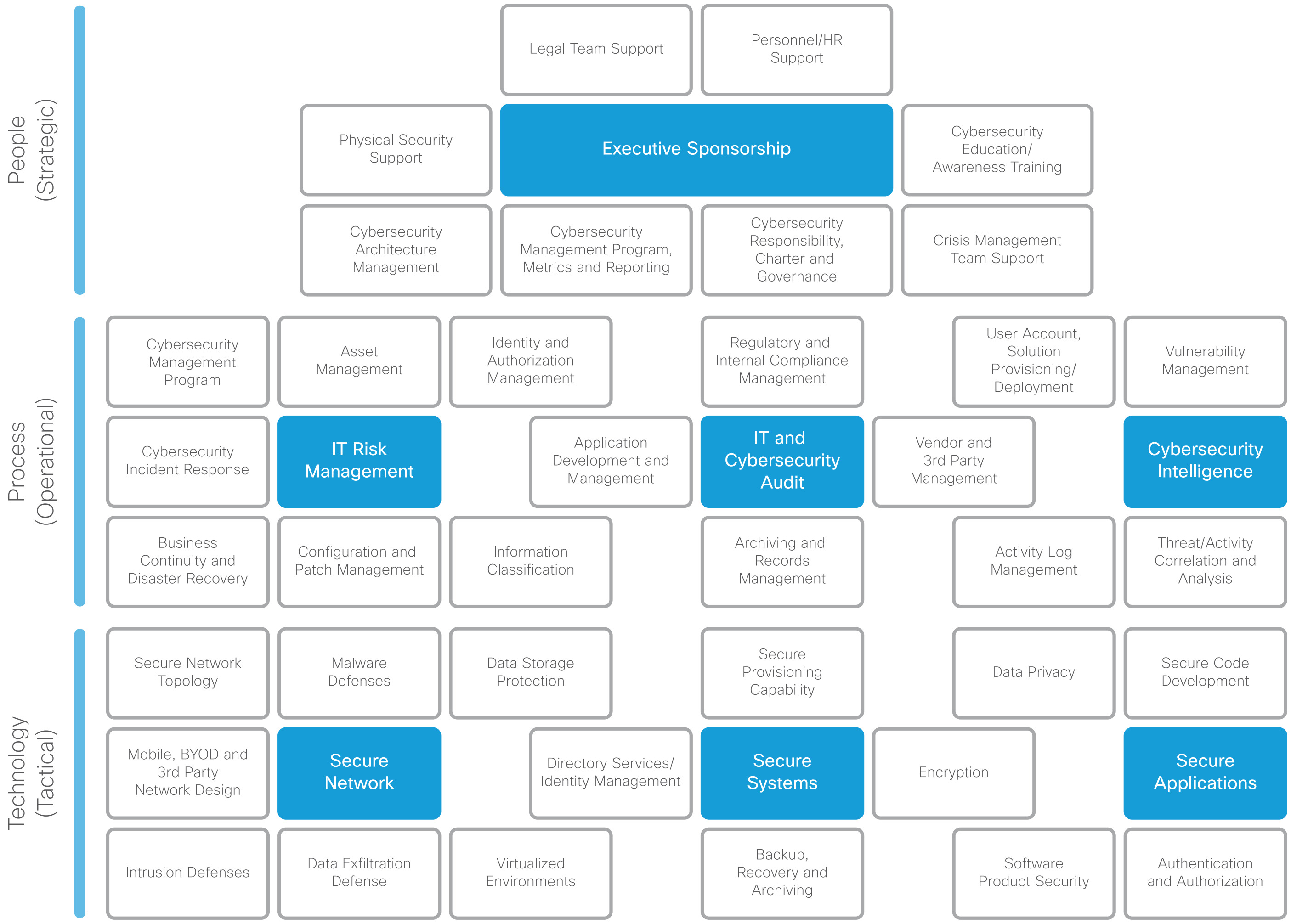
Although addressing cybersecurity challenges with only these layers is perfectly possible, adopting and using it in that way is difficult and potentially prone to error or misinterpretation. To ease such issues, you must divide these higher-level layers into more manageable chunks. The CMF subdivides its three macro layers into seven discrete focus areas:

- **Executive Sponsorship:** Key accountability required to drive the program
- **IT Risk Management:** Required to identify, monitor, and address cybersecurity risks posed to the organization
- **IT and Security Audit:** Required to ensure that IT and cybersecurity teams, and an organization’s user population are using information and IT resources appropriately
- **Security Intelligence:** Required to ensure IT and cybersecurity practitioners, and management are aware of both internal and external threat landscapes to further prevent or minimize the introduction of additional security-related risk to their organizations
- **Secure Network:** Required to design, implement, and manage network devices, appliances, other core components, communications channels, and management tools, whether physical or virtual, to protect the organization’s critical business assets

- **Secure Systems:** Required to design, implement, and manage computing systems, applications, and management tools, whether physical or virtual to protect the organization's critical business assets
- **Secure Applications:** Required to establish and monitor security controls, and secure operational features embedded in, or configured during, application deployment, whether physical or virtual to protect organizations' critical business assets

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. This tertiary layer requires the introduction of 38 cybersecurity elements as shown in Figure 1:

Figure 1: Cybersecurity Management Framework



People (Strategic)

Legal Team Support
Personnel/HR Support
Physical Security Support
Executive Sponsorship
Cybersecurity Education/ Awareness Training
Cybersecurity Architecture Management
Cybersecurity Management Program, Metrics and Reporting
Cybersecurity Responsibility, Charter and Governance
Crisis Management Team Support

Process (Operational)

Cybersecurity Management Program
Asset Management
Identity and Authorization Management
Regulatory and Internal Compliance Management
User Account, Solution Provisioning/ Deployment
Vulnerability Management
Cybersecurity Incident Response
IT Risk Management
Application Development and Management
IT and Cybersecurity Audit
Vendor and 3rd Party Management
Cybersecurity Intelligence
Business Continuity and Disaster Recovery
Configuration and Patch Management
Information Classification
Archiving and Records Management
Activity Log Management
Threat/Activity Correlation and Analysis

Technology (Tactical)

Secure Network Topology
Malware Defenses
Data Storage Protection
Secure Provisioning Capability
Data Privacy
Secure Code Development
Mobile, BYOD and 3rd Party Network Design
Secure Network
Directory Services/ Identity Management
Secure Systems
Encryption
Secure Applications
Intrusion Defenses
Data Exfiltration Defense
Virtualized Environments
Backup, Recovery and Archiving
Software Product Security
Authentication and Authorization

Cybersecurity Management Framework Adoption and Usage

The 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 operate their businesses (that is, generate revenue) to maintain their relevance.
In that light, is it possible that many may choose an unplanned approach, addressing isolated security challenges versus adopting such a framework? Truthfully, it is likely some organizations may proceed in that manner. If so, what is the point of a cybersecurity management framework?

Realism Sets In

The 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 frameworks. 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 management program based on a formal cybersecurity management 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.

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 objectives. 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 the SLT. 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, but also essential. Protecting these information assets is a responsibility everyone shares.

As the SLT defines the strategic way forward, stakeholders must evaluate and manage the risks associated with compromise, loss, or theft of information. A core SLT objective is to minimize business risk to acceptable levels–or eliminate risk altogether. Is it possible for an organization to completely eliminate all risk? While it is possible, 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 management 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, 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 the cybersecurity management program's policy definition.

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 cybersecurity program. Any organization is able to, and should, commit to a business-focused cybersecurity management program addressing SLT concerns as mandated, endorsed, and expressly articulated in the cybersecurity charter and policy.

Transforming an Existing Cybersecurity Management 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 management program.

Initially, IT and cybersecurity teams own responsibility for reviewing existing cybersecurity standards and processes. They are responsible for determination of whether documented requirements comply with 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. 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 management program that does not satisfy SLT-defined requirements. Prudent organizations should properly assess their cybersecurity management 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 while continuing to manage an acceptable level of risk. 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, be overly expensive, be slower to achieve, 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.

> Without such preexisting programs in place, transitions are typically too burdensome and likely will result in a cybersecurity management program that does not satisfy senior leadership team defined requirements.

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 this CMF adapted the Carnegie Mellon University (CMU) Capability Maturity Model (CMM) to better suit cybersecurity management programs. Carnegie Mellon University 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 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 elements associated with a given focus area. The focus-area's maturity scores can then be combined to provide an overall maturity score for the CMF layer and finally convey an overall cybersecurity management program maturity level.

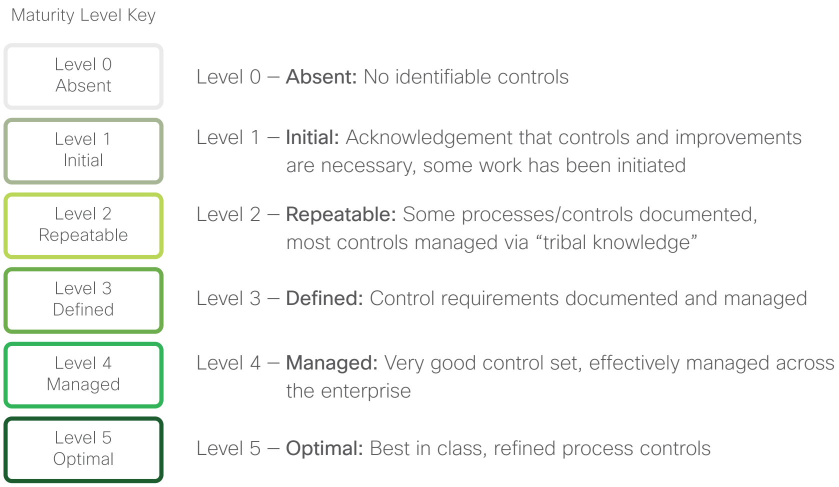
In practice, the authors of the CMF have experienced that most organizations using this approach usually ignore layer-level and total program-maturity scores and concentrate solely on the focus area and individual cybersecurity element maturity scores. This is most likely because responsibility for specific 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.

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

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 CMF are summarized in Figure 2.

Figure 2: CMF Maturity Levels



Level 0 – **Absent:** No identifiable controls

Level 1 – **Initial:** Acknowledgement that controls and improvements are necessary, some work has been initiated

Level 2 – **Repeatable:** Some processes/controls documented, most controls managed via "tribal knowledge"

Level 3 – **Defined:** Control requirements documented and managed

Level 4 – **Managed:** Very good control set, effectively managed across the enterprise

Level 5 – **Optimal:** Best in class, refined process controls

Every element in the CMF contains multiple sub-elements, each of which is associated with a pre-defined 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 management program best address everyone's needs.

The introduction of a CMP affects virtually every individual or group in an organization, so it is essential that the final cybersecurity management program best address everyone's needs.

Cisco Services' experience in developing CMPs indicates there 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 enterprisewide cybersecurity management 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, or higher.
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 use of a document review and version management system to support ongoing management of CMP documentation.
5. Complete work on the Cybersecurity Management Framework's strategic elements first. Note: 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. Develop all remaining elements having dependency on key elements followed by elements having no dependencies. Ensure all documented elements for consistency, accuracy, and elemental dependencies.
9. Ensure all current and future security-related initiatives to the agreed upon by the organization's crisis management team are taken into consideration and included in the appropriate CMF elements.
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 management 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 benefit that organizations achieve through development and implementation of such programs based on a strong cybersecurity management framework is consistency and reduced instances of successful cyber attacks. Moreover, a cybersecurity management program often reduces a successful attack's impact on an organization's bottom line due to its programmatic predefined approach for identifying and responding to cybersecurity incidents.

As a trusted partner, Cisco Security Services can assess the maturity of your CMP and, if required, help you improve your CMP, or create and deploy a CMP tailored to your organization's needs, based on a proven Cybersecurity Management Framework. The resulting program will be developed using expertise and experience gained from assessment and development of numerous CMP initiatives across different industries.

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