INFORMATION SECURITY PROGRAM ESSENTIALS

A GUIDE PRODUCED BY THE TEXAS CISO COUNCIL

VERSION 1

APRIL 19, 2015

CONTENTS

Executive Summary 3
Using This Guide 5
Contributors 5
Governance and Organization 6
Information Security Strategy 11
Information Security Framework 20
Information Security Risk Management 25
Measurement and Metrics 30
Glossary 35
License 37

EXECUTIVE SUMMARY

THE COUNCIL

The Texas CISO Council is a group of Texas-based information security leaders who have real-world experience managing information security corporate or governmental functions, or have made substantive contributions to the information security industry. These volunteers represent various organizations and are motivated by sharing ideas, acknowledging successful industry practices, and promoting information security in both the public and private sectors. The contributions of members of the Texas CISO Council do not reflect the policies of their employers, and the guidance contained in this Guide should be adapted to an organization's specific policies and legal compliance requirements. This Guide is offered at no cost or obligation to any organization that seeks to build or improve their information security program. This document should be utilized in conjunction with supplemental resources located at www.texascisocouncil.org.

PROBLEM STATEMENT

There are many similar and overlapping information security control frameworks in place around the globe. Examples include *Information technology – Security Techniques – Code of Practice for Information Security Management* (ISO 27001/2), The Information Security Forum (ISF) *Standard of Good Practice for Information Security*, and the National Institute of Standards and Technology (NIST) 800 series publications. Although these frameworks abound and are quite comprehensive, there is no simplified reference describing at a high level the essential components of a modern information security program. In most cases, it is difficult to get started when designing, refining, or measuring an information security program. As program leaders, we are often forced to blaze our own unique trail in the pursuit of stronger security and better protection of our organization's information resources. This Guide will help new and existing programs build more consistently successful practices.

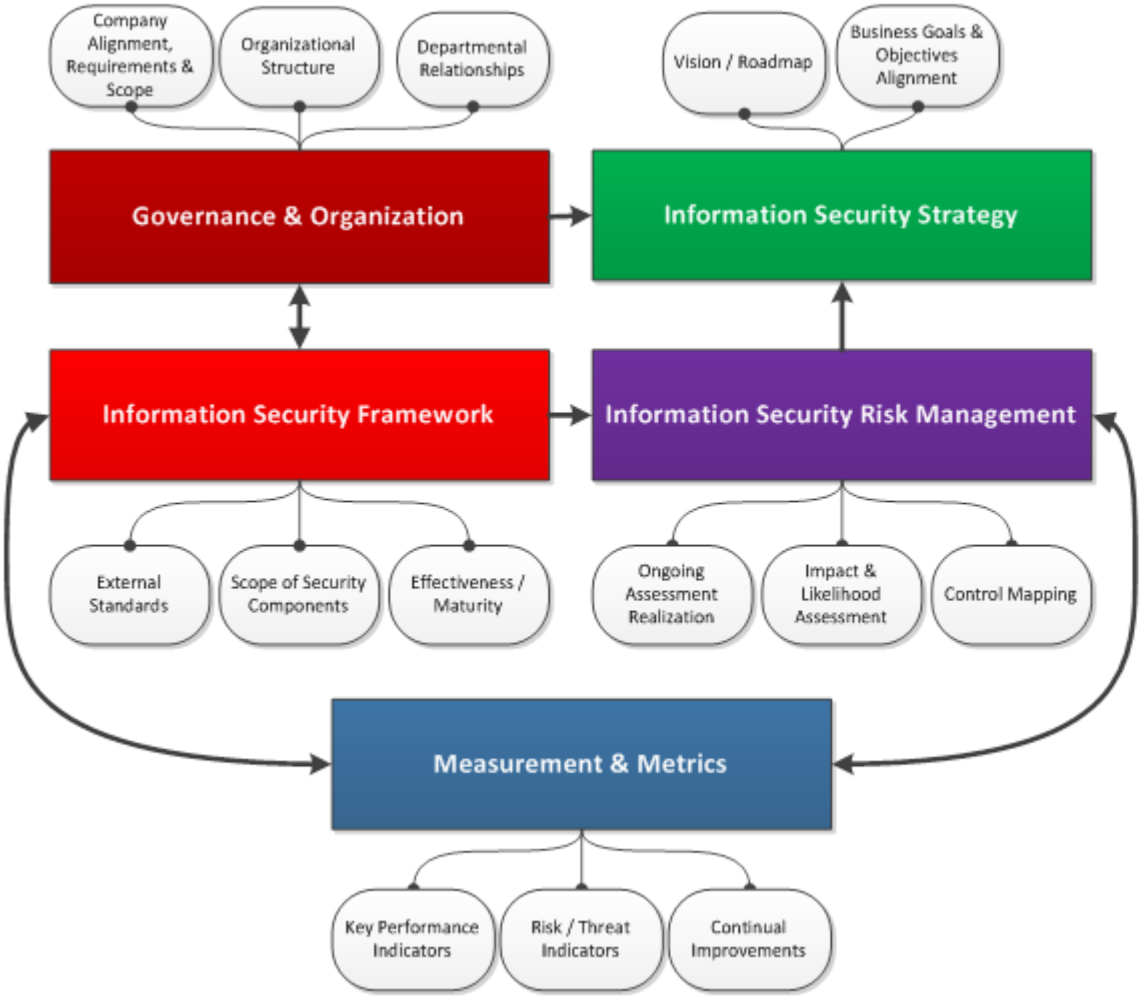
The primary goal of creating this Guide was to offer a simplified mechanism to validate that an organization has in-place or planned solutions for key elements of an information security program and that the organization has not overlooked critical core competencies or controls. The Guide may also aid an information security professional or business leader to document an approach, support peer reviews, and/or allow a security program owner to present program fundamentals to internal stakeholders, auditors, partners, and vendors. Without a common frame of reference, benchmarking security programs can be challenging. Program assessments against the core components described in this Guide may also allow organizations to compare and contrast their information security programs with similar organizations.

PROPOSED SOLUTION

The Texas CISO Council collectively defined five core components that should be part of an effective information security program. These include:

- **Governance and Organization**
- **Information Security Strategy**
- **Information Security Framework**
- **Information Security Risk Management**
- **Measurement and Metrics**

Each of the five components is further defined in the graphic below and is explained in greater detail in the following sections of this Guide. In addition, each component has an inherent relationship with the others. Therefore, each section can provide an input and/or output to another section. Readers should take into consideration that in most cases, information security programs must have some capabilities in each of the five components (at varying maturity levels) to be considered effective.


Company Alignment, Requirements & Scope
Organizational Structure
Departmental Relationships
Vision / Roadmap
Business Goals & Objectives Alignment
Governance & Organization
Information Security Strategy
Information Security Framework
Information Security Risk Management
External Standards
Scope of Security Components
Effectiveness / Maturity
Ongoing Assessment Realization
Impact & Likelihood Assessment
Control Mapping
Measurement & Metrics
Key Performance Indicators
Risk / Threat Indicators
Continual Improvements

USING THIS GUIDE

Readers of this Guide should familiarize themselves with all of the five core component sections prior to designing, modifying, or measuring their information security programs. An understanding of the core components and their interdependencies can add value to an information security program of any size. As information security is a dynamic and ever-changing environment, readers should also consult supplemental resources and possible updates at www.texascisocouncil.org.

This Guide contains a Glossary of common security-related terms as well as references throughout the text for additional background and context.

Readers are encouraged to provide feedback on this Guide by email to info@texascisocouncil.org.

CONTRIBUTORS

The Texas CISO Council would like to thank the following individuals for their contributions to the development of this Guide. More information on all of the Council members is available on the website.

Philip Beyer
Director, Information Security
The Advisory Board Company

Mary Dickerson
CISO
University of Houston System

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Parrish Gunnels
CISO
Invitation Homes

Roger Hale
CSO Veritas
Symantec Corporation

Shawn Irving
Vice President and CISO
Michaels Stores Inc.

Joseph Krull
Director
Denim Group

Joe Oranday
SVP, Enterprise Information Security
Financial Services Industry

Joel Scambray
Managing Principal
Cigital

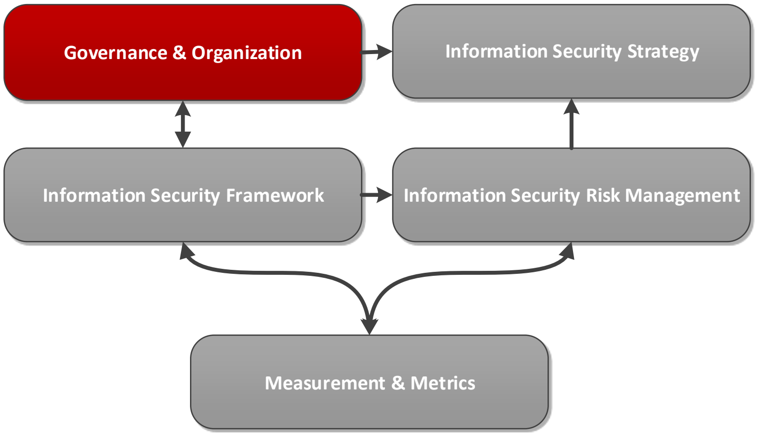
John South
EVP and Chief Security Officer
Heartland Payment Systems

Greg White, Ph.D.
Director, Center for Infrastructure Assurance and Security
University of Texas at San Antonio

Brian Wrozek
CSO
Alliance Data

GOVERNANCE AND ORGANIZATION

OVERVIEW


Governance & Organization
Information Security Strategy
Information Security Framework
Information Security Risk Management
Measurement & Metrics

The term “information security” can mean different things in different organizations and with different people depending on their experience and their perception of security. The information security team and function can be organized in many different ways, depending on how an organization views its external and internal threats and its overall security posture. When discussing security governance and organization, one of the most common questions surfaces - where does information security report within the overall organization? The answer to this question also guides decisions, which will be made regarding the necessary governance structures that need to be in place to support successful execution of an effective information security strategy within the organization.

AUDIENCE

- The primary audience for matters related to security governance and organization should be the organization's executive leadership team. Due to their overall responsibility to the organization, the team must endorse and support the structure of the information security program and governance processes.
- The entire organization should understand the information security program structure, authorities, governance processes, and their individual responsibilities as employees to protect sensitive data and support information security functions.

COMPONENTS

ORGANIZATIONAL STRUCTURE

When evaluating where information security should fit within the company structure, stakeholders should consider the following factors:

- The desired level of visibility within the organization for information security issues
- Customers of the information security program, both internal and external
- The organization’s perception of information security risks - significant to organizational objectives, or primarily as IT-centric concerns

- Objectives for the information security program, i.e. is the program primarily designed to meet compliance requirements only, or is information security responsible for broader aims
- Is the designated owner of the information security function (e.g. Chief Information Security Officer [CISO], Security Director, or other designated position) responsible for information security functions across the entire organization, or only for specific business units or territories

COMMON STRATEGIES

- **Information Security as part of the IT function** – In this model, the information security program leader (i.e. CISO, Security Director, or designated owner of the information security function) typically reports to the CIO. Benefits include a tight working relationship within IT. In smaller organizations, the CISO may also assume an operational role – combining information security with network service management.
  <u>Executive Sponsor: CIO</u>
    - *Visibility within the organization for information security issues* - Low (as information security will generally be seen as a subcomponent of broader IT issues)
    - *Customers* - Primarily internal to IT with limited external customers
    - *Organization perception of information security risks* - IT-centric concerns
    - *Objectives for the information security program* - Primarily focused on compliance and tactical/operations-oriented objectives
    - *Authority for the information security program leader* - Primarily recognized specific to individual business units
- **Information Security as part of the risk management/compliance/privacy function** – In this model, the information security program leader typically reports to the position with overall responsibility for Organizational Risk Management, Compliance, and/or Privacy. In many cases, this might be an organization's General Counsel, head of the internal legal department, or Internal Audit. Benefits include a champion for information security issues outside of the IT operations environment.
  <u>Executive Sponsor: General Counsel or Chief Risk/Privacy Officer</u>
    - *Visibility within the organization for information security issues* - Medium
    - *Customers* - Primarily external to IT
    - *Organization perception of information security risks* - Focused toward organizational risk management goals
    - *Objectives for the information security program* - Focused on compliance
    - *Authority for the information security program leader* - Generally recognized across the organization
- **Information Security as part of the converged Security function** – In this model, the information security program leader's role may be combined either functionally or strategically with physical security responsibilities. Benefits include converged approaches to security matters.
  <u>Executive Sponsor: COO, CEO, CFO</u>
    - *Visibility within the organization for information security issues* - Medium

  - *Customers* - Primarily external to IT
  - *Organization perception of information security risks* - On par with physical security issues
  - *Objectives for the information security program* - Focused on meeting specific business needs
  - *Authority for the information security program leader* - Potentially recognized broadly across the organization
- **Information Security as a strategic business driver** – In this model, the information security program leader typically reports to the CEO/Board of Directors. Information Security is seen as a business enabler; a critical factor in achieving a competitive advantage for the organization.
  Executive Sponsor: CEO or Board Chairman
  - *Visibility within the organization for information security issues* - High
  - *Customers* - Primarily external to IT
  - *Organization perception of information security risks* - Significant to organizational objectives
  - *Objectives for the information security program* - Critical factor toward achieving a competitive advantage for the business
  - *Authority for the information security program leader* - Recognized broadly across the organization as a significant component in the success of the organization

RECOMMENDED PRACTICES

The Texas CISO Council recommends the following steps to properly align the Information Security organization within the company's overall structure:

- Formalize a common definition of security and risk governance in your organization.
- Define and implement an information security and risk governance function that is integrated with the organization's corporate and IT governance functions.
- Focus on the governance processes and functions, rather than on the organizational position of the activities.
- Establish a consistent channel of communication within your organization to speak on how the security program contributes to the organization's mission.
- Attempt to create an effective program regardless of where you sit in the organization.
  - If you are not placed in the proper organization structure, what should you do? Strategies:
    - Find your champions by gaining allies in your organization
    - Build cross-functional relationships outside of IT
    - Show your value
- Identify security advocates outside of your reporting structure to help you promote information security across the organization and gain consensus.
- Define how information security risk should be tracked, presented, and communicated.
- Tailor the information security program (where appropriate) with different business units by understanding their unique risks and processes.

- Regularly benchmark your information security program with peer and non-peer companies to identify any potential gaps, and to reassure organizational management that reasonable diligence is occurring. Ideally this is done formally, but informal approaches can also work.
- Consider creating an overall objective or mission statement for your information security program that is closely aligned with organizational imperatives and is understood/approved by key stakeholders. Continuously adapt the mission statement to the organizational direction, and align the information security program with it ongoing.

CORE COMPONENTS OF INFORMATION SECURITY PROGRAMS

- Security Operations/Tactical - Day to day use of the technologies and processes in place to support the business; examples include use of intrusion detection/prevention technologies, network and application vulnerability scanning, incident management (monitoring, response, and reporting), forensics, and compliance management (monitoring compliance with information security activities required to meet industry/state/federal/regulatory/organizational policy requirements)
- Security Engineering/Solutions Architect - Evolution and support of underlying technology platforms that provide services; includes advising project teams (internal/external) in the adoption and integration of security services necessary to support initiatives
- Secure Software Development Lifecycle (SSDLC) - Integration of security checkpoints and activities into the software development process
- Identity and Access Management
- Awareness and Communications to both Employees and Customers
- Policy, Procedures, and Process Controls
- Metrics and effectiveness performance monitoring
- Governance/Accountability reporting
- Project Integration - Security design, architecture, and review

DOCUMENTATION

- Define and document the scope of your security program:
    - Cross-functional responsibilities
    - Localization (regional/geographic areas)
    - Recognition of information security functions outside of the designated information security team (if appropriate), such as through virtual or matrixes relationships, or ad hoc situations
- Identify the employees or third-parties assigned to information security functions
    - Internal resource (full-time staff, part-time staff, dedicated, or matrix)
    - Third-party/outsourced resources
- Identify and document the financial resources/budget allocated to security functions
- Identify actions necessary to secure funding to address extraordinary security needs

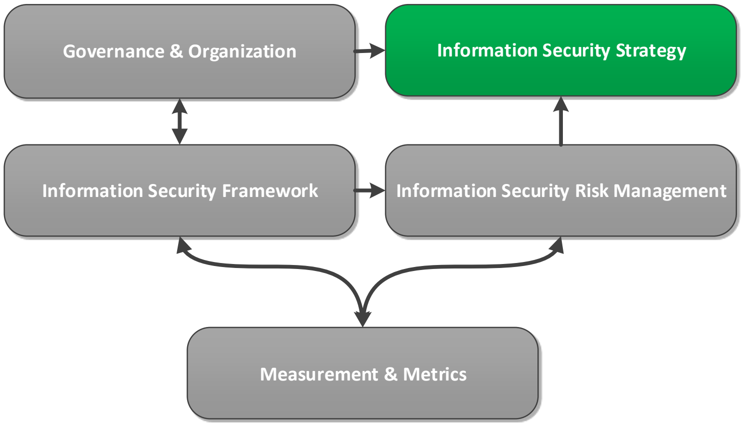
- Define the accountability/relationship of staff outside of the information security group that perform functions directly or indirectly related to information security
- Document the mechanisms used to align security program strategy with organization strategy
- Define and document the methods used to manage performance and continual improvement of operations
- Identify how risk decisions are made in relation to information security
- Document the level at which risk decisions are known, understood and accepted by the executive management of the organization
- Define how information security considerations and controls are integrated into emerging projects/initiatives, both internal and external to enterprise IT
- Define and document the key stakeholders: Legal, Audit, etc. and the methods used to strengthen relationships with these areas
- Identify how organizational culture drives the execution of security operations

RESOURCES

Webinar - Tom Scholtz, Gartner, "Build An Effective Security and Risk Governance Function" - http://www.gartner.com/webinar/2745217

INFORMATION SECURITY STRATEGY

OVERVIEW


Governance & Organization
Information Security Strategy
Information Security Framework
Information Security Risk Management
Measurement & Metrics

The purpose of creating an information security strategy is to define a plan, typically from one to three years, for meeting the organization's security objectives. For example, an organizational objective might be to ensure the confidentiality, integrity, availability, and compliance of information contained in business systems**.** The information security strategy should be aligned with the organization's overall business strategy.

Confidentiality: Ensuring that access to sensitive data is restricted to the people, processes or technology that has a legitimate need for that access

Integrity: Maintaining and assuring the accuracy and consistency of data over its entire lifecycle in order to have confidence that your information is accurate and systems are functioning as expected

Availability: Assurance that information and systems are available when needed

Compliance: Making sure people and systems continue to conform to the given security requirements over time

It is the responsibility of the security leader to ensure that the information security program accomplishes the following goals:

1. Supports and enables business objectives
2. Reduces risks to levels acceptable by management
3. Ensures compliance to regulatory and industry requirements

> Developing a security strategy is less of a science and more of an art.

When one analyzes the many ways that the security of an enterprise can be compromised, it is difficult, at best, to match the company's resources against the skills and toolsets that the malicious actors have at their disposal. However, the life of a company may be defined by how well they can identify, respond, and mitigate the various threats facing them in cyberspace.

Since there is no such thing as perfect security, the security strategy should include detective and reactive measures in addition to protective solutions. Trained people, mature processes, and security specific technologies should be part of your security strategy to various degrees. This section of the Guide is not meant to be an exhaustive list of everything that should be included in your overall security program. It should be used to help you develop your security strategy.

The first, and possibly the most important lesson to take away from the security discussion, is that security is not a one-time process. As your business goals and threats facing your business change, your security strategy must be reviewed and modified if necessary. It should be a living security strategy geared towards actively protecting the enterprise, rather than a compliance-driven function that is dusted off once a year for review.

The information security strategy should be widely communicated to senior management, key stakeholders, and members of the organization. The strategy should be created and updated to closely synchronize with the organization's overall business strategy. For example, if your organization plans to enter new markets or geographic areas and those areas would incur additional risk, your security strategy would reflect what advanced controls or processes you'd plan to implement to match that business decision.

AUDIENCE

The primary audience for the security strategy is senior management, which includes your peers up to and including the Board of Directors. Your security strategy may need to be shared with trusted third-party company executives including suppliers and customers if they are tightly integrated into your business model. In highly regulated industries such as financial services and healthcare, external auditors and regulators may need to be updated on your security strategy. Your short-term projects and priorities flow from your security strategy to move the security program forward.

COMPONENTS

Key Action: First and foremost, the security strategy must be aligned with the business strategy. Before you do anything else, you must understand your business. Even the best security strategy will fail if it doesn't enable the attainment of business objectives and have management support.

STRATEGIC FACTORS

Inputs into the security strategy development process come from multiple sources but they can be grouped into the following categories:

- Internal Factors
  - You need to understand the strategy and priorities of your various business units and supporting departments like IT and HR. Your security strategy must align with their activities and support the attainment of their goals.

  - You must have thorough knowledge of the overall technology environment. Partner with IT to understand the network topology. Obtain an inventory of all hardware and software assets, including their security requirements and status. Learn how data flows throughout your company and how it is shared with third parties and service providers.
  - Assess the culture and risk appetite of the company. This can often be accomplished through conversations with business representatives at various levels within your organization.
- External Factors
  - You must stay up to date on the latest threats and changes in regulations in order to determine if they impact your business and security posture. Security is a dynamic environment that needs to be constantly updated.
  - In some cases, you may have specific customer requirements to meet and these may need to be taken into consideration as you develop your security strategy.
  - Technology continues to advance and evolve. You must continue to evaluate potential solutions and how these could improve your security program.
- Self-Guided Factors
  - It is recommended that you routinely evaluate your security program to identify gaps and opportunities for improvement. Your security strategy should address these gaps based on the level of risk your company is willing to take.

While learning about all these factors themselves may happen simultaneously, the final analysis and priority build-out typically happens in the following order:

1. Business priorities come first. Determine if new security activities are required or if changes need to be made to existing solutions in order to enable them.
2. IT priorities typically come next. Again, determine if new security activities are required, or if changes need to be made to existing solutions in order to enable them. Follow this same approach for other internal departments including your suppliers and customers as needed.
3. Based on research, determine if any new regulatory or industry compliance requirements need to be met.
4. Evaluate new risks and threats to see if your existing security strategy sufficiently addresses them or if you need to make changes.
5. Complete your security strategy by addressing your most pressing needs based on your own analysis from various self-assessment activities.

INTERNAL FACTORS

> The best way to learn about the priorities of your business units and support organizations is through collaborative activities.

This can be done through formal means like asking them to fill out a survey, attending their staff meetings or by joining various cross-functional committees. You can also obtain this information informally by simply asking managers probing questions or reviewing internally published documentation regarding their activities. The more you know about their business priorities, the better you can tailor your security strategy to gain their support. As you start to formulate your security strategy, seek out feedback from peers to ensure alignment.

Many companies struggle with maintaining a detailed IT asset inventory, a mapping of network connectivity and data flow diagrams. These resources are essential to an efficient information security program and an effective security strategy. You should assist your IT team as much as possible to create or refine these materials.

Aligning your security strategy with the company culture and risk appetite is a difficult task. There is no easy way to describe how to achieve this alignment but getting feedback on your security strategy from different stakeholders will help you determine if you are on the right path. Communicate your proposed security strategy and any fundamental changes widely and often. Be prepared to modify your strategy based on valid input from your organization and senior management.

EXTERNAL FACTORS

Major security events such as large data breaches may have an impact on your security strategy. It is important to stay current on external events and trends via dedicated research activities and daily reviews of security related information. There are many providers of security related news including mainstream print and electronic media, security industry materials, and selected social media sources. Examples of specific sources of topical information security subjects include the SANS Institute, SC Magazine, Wired Magazine, and Security Focus.

SELF-GUIDED FACTORS

There are multiple ways to assess gaps in your portfolio or identify potential improvements in your security program as you develop your security strategy. A few are discussed in this section.

PROTECT - DETECT – RESPOND

One approach that has grown in popularity is to evaluate your program using the “Protect – Detect – Respond” triad to ensure that you have sufficient controls in all three areas.

PROTECT

You must establish a protection plan that implements a combination of technologies, processes and policies geared towards protecting the assets and data of the enterprise. The foundation for protection is access control.

In smaller organizations, protection may be simply a firewall with its associated access control list. In more complex organizations, the protection may encompass a system of firewalls and their respective access control lists, a more intricate network infrastructure consisting of demilitarized zones (DMZs) to isolate external facing assets, VLANs to further isolate parts of the network through segmentation and processes such as encrypting sensitive data at rest and in transit. Another important protection initiative is to ensure that security is “built in” to software or technology that the organization produces, whether for internal or external use.

The most important aspect of the protection plan is to understand what assets comprise your networks. An accurate inventory of computers and laptops used by the members of the enterprise is the first step. Who has been issued what devices? Is there an approved software load for those devices (a baseline image)? Does the image include a hardening protocol to ensure that all patches are applied and all of the software that protects the computer (e.g. anti-virus) are implemented and connected to their respective control monitors? It is also important to make sure that all of the critical assets are properly configured to generate and transmit log data, particularly if your organization uses a Security Information and Event Management (SIEM) platform. Log data allows you to investigate anomalies and determine sources of real or potential data breaches.

DETECT

As with the protection plan, a detection strategy is an important component of your security strategy. The foundation for the detection program is established in your protection plan as the two really go “hand-in-glove”. Once again, you must have an accurate inventory to ensure that your detection plan encompasses all of the enterprise assets (computing assets as well as infrastructure assets). You also need to ensure that the tools implemented as part of your protection are correctly installed and configured. They should be actively reporting to their respective control monitors.

A detection tool that may come into play for your organization is a Security Information and Event Manager (SIEM). The SIEM will collect all of the event data that is fed from your infrastructure and computing devices. These logs are very important, as studies have shown that indicators of most breaches were present in the logs of the enterprise assets before the breach was identified.

Interestingly, many companies implement the tools needed to do the detection necessary to stop an attack in its tracks. However, as seen in the news regarding some of the most prominent retail breaches, the tools were in place in many of those cases, but there was a breakdown in the alerting process. This may have had a large impact on the success of the attacks.

RESPOND

Response is critical to the success of your security strategy as is prevention and detection. As mentioned above, having the prevention and detection tools in place but not having an effective incident response program could completely nullify the benefits of your other efforts.

ESTABLISH AN INCIDENT RESPONSE POLICY AND PLAN

Establish a policy that defines how incidents will be declared and handled. In addition to “day-to-day” incidents, how are incidents of a more severe nature escalated. Incident response policies can be a simple or complex, as you need to handle your environment. There are many examples of incident response policies and plans tailored to various industries on the Internet. Find one that can be worked into an operational incident response strategy for your enterprise.

ESTABLISH AN INCIDENT RESPONSE TEAM

An incident response team should be established to execute an incident response plan effectively. More importantly, the team must practice incident response drills fairly regularly to be able to react instinctively during a real incident, particularly one that would be considered a major incident such as a breach of the systems that house your sensitive data. You should conduct simulated breach exercises involving members of your organizations' managements at least annually (or more often if your organization processes sensitive customer information).

LESSONS LEARNED

> Follow up every incident, whether practice or the real event, with a "lessons learned" exercise.

It is seldom the incident response team and the support personnel that assist in an incident don't learn something that would improve the response process for the team, or improve the business or technical processes that failed and resulted in the incident. By tracking your incidents over time, you can look for any patterns or other insights that may help you adjust your security strategy based on tangible events to your company. These incident case studies are very helpful when making your case for new security investments.

KILL CHAIN MODEL

A more advanced, systematic approach involves the Cyber Kill Chain® model (See Figure 2: Lockheed Martin Cyber Kill Chain Model). In a nutshell, the kill chain model was defined in a paper on Intelligence-Driven Computer Network Defense, and it was first published at the 6th Annual International Conference on Information Warfare & Security in March 2011. The authors define the seven stages that an attack must complete in order to accomplish a compromise of a company. It is impossible to stop all intrusions but you can disrupt the attack anywhere along the chain thereby preventing the loss of your information.

In addition to the stages of an attack, there is a spectrum of six courses of action that can be deployed to stop an attack at each of the seven stages:

- Detect the attack
- Deny the attack
- Disrupt the attack
- Degrade the attack
- Deceive the attacker
- Destroy the attack

A detailed matrix of the courses of action for each link of the chain can be created and evaluated against your security posture to help you determine where you need to apply more attention. Further information about the Cyber Kill Chain® Model can be found in the paper referenced in the footnote. The model tells us the sooner in the model you identify an attack, the more likely you are to stop the attack before the malicious actor can complete a compromise of your data. The contention is also made in the model that the sooner you detect and stop the attack, the less costly it will be for the entity and the more costly for the attacker.

THIRD-PARTY ASSESSMENT

Another common approach is to engage a third-party to conduct an assessment of your security program. There are many security and audit companies that can perform this service for you. While you can do this evaluation yourself, it is often good to get an independent view of your program. Employing a neutral third-party eliminates any biases you may have and increases the credibility of the findings. If you find using a third-party cost prohibitive, you can set up a rotation schedule. Have the third-party conduct the assessment every three years, and then update it yourself in the intervening years. You may also consider using the resources of your Internal Audit department to assess portions of your information security program.

As part of this assessment, you can compare your security program to an industry framework such as ISO 27001/27002. There are other resources can be used such as the SANS Top 20 Critical Controls. Many vendors will provide a 1-5 point score similar to the Carnegie Mellon Maturity Model or at least a basic High/Medium/Low or Red/Yellow/Green format. Don't get hung up on trying to select the perfect framework. Have your program assessed with a framework that resonates with you and your stakeholders and don't be afraid to tailor it to fit your company profile.

CONSIDERATIONS

You may want to evaluate the pros and cons of obtaining cyber insurance. Cyber insurance is going through a period of resurgence and many organizations are adding this capability to their information security programs as a way to reduce the monetary impact of a security breach.

Managed Security Service Providers (MSSP) are also used by many organizations as a component of their information security strategy. MSSPs can provide skilled resources to supplement your existing security staff.

A recommended practice is to update your strategy at least on an annual basis. The Texas CISO Council recommends that you have a high-level, multi-year plan in addition to a detailed yearly plan. Both the long-term and short-term items should be reviewed and updated. Ideally, this update should occur before your yearly budget cycle so you can include the financial impact of your strategy in your budget plans. You will need to circle back and update your strategy based on the final approved budget since you may not have all the funding for everything you hoped to accomplish. Having the documentation that shows what was originally planned and what was ultimately funded and approved is important in the event that something happens in the future.

Some elements of your strategy, such as maintaining regulatory compliance may rarely change from year to year while other items like your actual priorities and budget may change dramatically. Security is a dynamic environment so you may expect a lot of changes. In fact, a good practice is to review your strategy mid-year to document your progress and determine if any adjustments need to be made. You should also review your strategy after major business changes such as those resulting from an acquisition.

You should account for the priorities, workload, and budget of other groups in your strategy. In many companies, the IT organization often manages and funds the hardware, software, and other solutions that your security strategy impacts. Therefore, you should aim to avoid overwhelming the IT organization with security activities since they have new projects, initiatives, and daily run/maintain efforts in addition to any security items.

Your security strategy needs to be flexible to account for other company activities and the normal ebb/flow of market conditions.

In most cases, management decisions will impact the direction of your security strategy but occasionally security will need to be proactive to make recommendations to management regarding the direction the company should take for a given situation. This is particularly important during acquisitions, changes in products and services offerings and expansions of business to new territories.

Use of the same security framework and renewing contracts with vendors year-over-year provides consistency and the ability to measure progress over time; however, this can lead to blind spots and complacency. Therefore, we recommend that you look at your security environment through multiple lenses. These different perspectives can often uncover hidden gaps or problem areas. For example, you may wish to examine specific components of your security program using elements of the ISO, ISF, or NIST framework and rotate vendors providing essential security services such as network vulnerability scanning or penetration testing.

RESOURCES

Figure 1: Strategy Development Flow

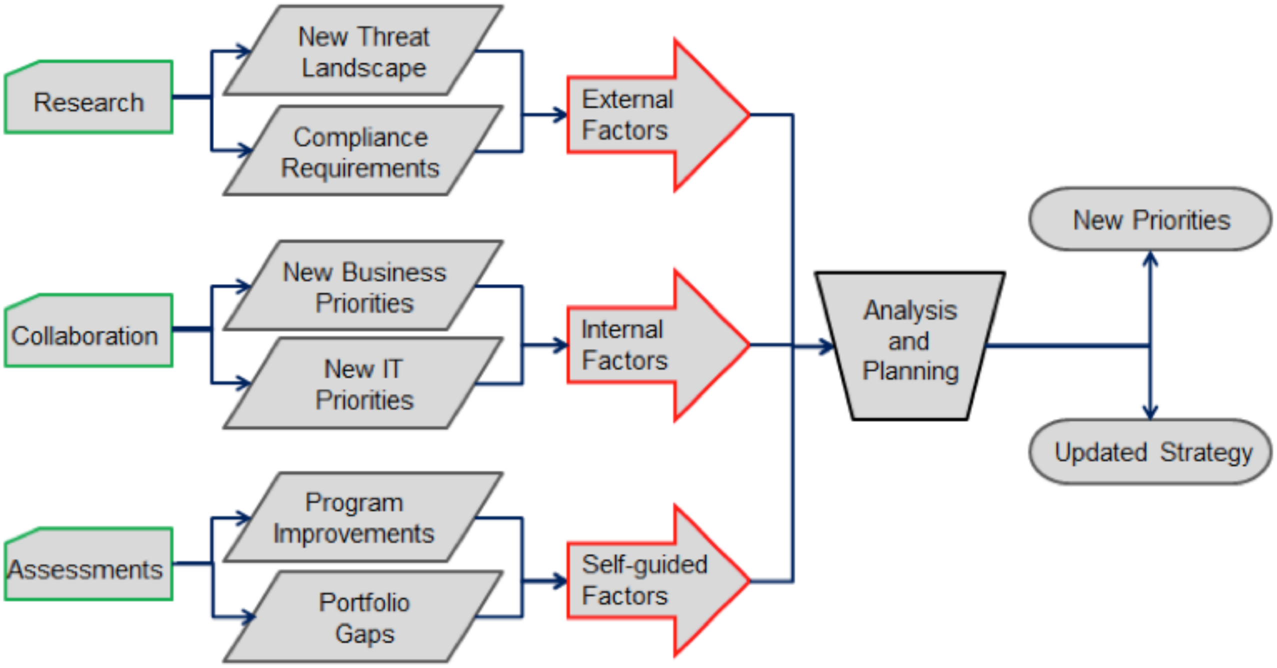
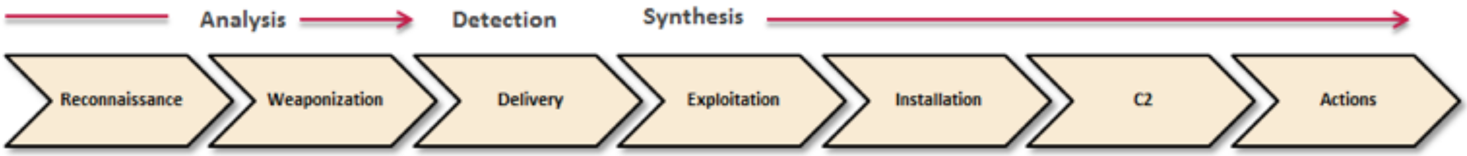


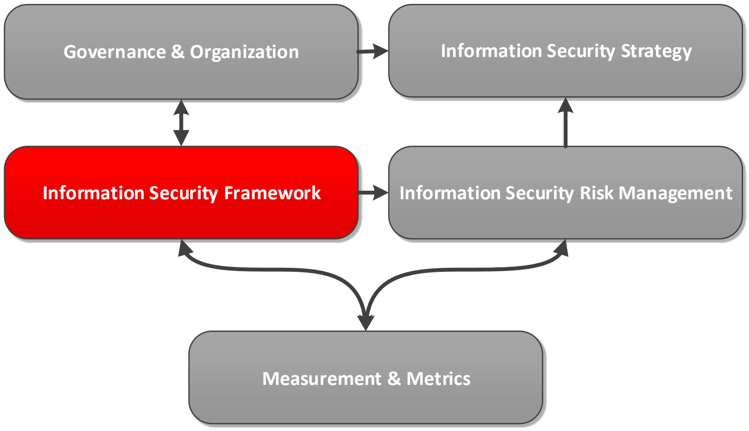
Figure 2: Lockheed Martin Cyber Kill Chain Model



Hutchins, Eric M., Cloppert, Michael J, and Amin, Rohan M. Ph.D., Lockheed Martin Corporation. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". URL: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, page 7

INFORMATION SECURITY FRAMEWORK

OVERVIEW


Governance & Organization
Information Security Strategy
Information Security Framework
Information Security Risk Management
Measurement & Metrics

An Information Security Framework is a defined set of components used to design, manage, and measure an information security program. An organization's Information Security Framework describes the industry standard framework(s) used by the security program or defines a custom framework if applicable.

An organization should consider choosing an industry standard framework as the basis for the ongoing management of security practices, activities, and objectives to ensure that the information security program has considered a comprehensive and complete approach.

Industry standard frameworks help provide the specific safeguards for managing risks that accompany the use of technology by the organization. Either through the selection and use of an individual framework or a compilation of frameworks in a hybrid approach, the effective implementation of an Information Security Framework will help the organization ensure compliance to regulatory requirements as well as provide the basis for defining comprehensive controls and safeguards for protecting against threats and managing risks.

AUDIENCE

The Information Security Framework and associated components are most commonly used by the following organizational audience members:

- Information Security Personnel and Direct Reports to the Information Security Program owner (i.e. the Chief Information Security Officer, Security Director, or other designated person)
- Auditors / Regulators
- General Counsel
- CIO and IT Personnel
- Service Providers / Vendors
- Trusted Business Partners

COMPONENTS

- Framework Selection Process – The decision criteria for determining the industry standard framework(s) that comprise the organization's Information Security Framework.

- Scope of Framework Application – The description of the generally recognized set of security program components selected and implemented within the organization, including which components of the framework are deemed in scope or out of scope, and reasoning for exclusion of de-selected framework components.
- Framework Role Assignments – The mapping of responsible parties for governance, oversight, and operational execution for distinct functions within the framework.
- Framework Assessment – Relates to the Program Measurements and Metrics to evaluate effectiveness of the Framework functions and associated controls that are defined.

FRAMEWORK SELECTION PROCESS

The framework selection process should include several organizational factors, including but not limited to:

- Domestic or International Business Operations
- Interaction with U.S. Federal Government entities
- Upstream Supplier and Provider Reliance
- Requirements of Downstream Relationships
- Business Compliance Requirements

INDUSTRY STANDARD FRAMEWORKS

- National Institute of Standards and Technology (NIST) Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* - http://dx.doi.org/10.6028/NIST.SP.800-53r4
- Information Systems Audit and Control Association (ISACA) COBIT 5 - http://www.isaca.org/cobit/pages/default.aspx
- International Standards Organization (ISO) 27001:2013 / 27002:2013 - http://www.iso.org/iso/home/standards/management-standards/iso27001.htm http://www.iso.org/iso/catalogue_detail?csnumber=54533
- The Information Security Forum (ISF) *Standard of Good Practice for Information Security* - https://www.securityforum.org/tools/sogp/

FRAMEWORK RESOURCES AND CHECKLISTS

- NIST / C3 Voluntary Framework for Improving Critical Infrastructure Cybersecurity - http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- SANS / Council on Cybersecurity Top 20 Critical Controls - http://www.sans.org/critical-security-controls/controls
- Texas Cybersecurity Framework Security Plan - https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/AgencySecurityPlanTemplate.xls

REGULATORY AND COMPLIANCE REQUIREMENTS

- IRS 1075 Safeguards for Federal Tax Information (FTI)

- Criminal Justice Information Systems (CJIS) Requirements
- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach Bliley Act (GLBA)
- Federal Financial Institutions Examination Council (FFIEC)
- The Children's Internet Protection Act of 2000 (CIPA)
- The Children's Online Privacy Protection Rule of 2000 (COPPA)
- Payment Card Industry Data Security Standard (PCI DSS) v3.0
- European Union Privacy Standards
- Texas Business and Commerce Code, Chapters 503 and 521
- Texas Health and Safety Code, Chapter 181 (Medical Records Privacy)
- Texas Health and Safety Code, Chapter 611, (Mental Health Records)
- Texas Penal Code, Title 7, Chapter 33 (Computer Crimes)
- Other state data privacy laws (as applicable to your organization)

SCOPE OF FRAMEWORK APPLICATION

Once the framework has been selected, the organization may determine that elements or controls within the framework are not deemed necessary. When the organization determines that framework elements or controls will not be applied, the decision process should be formally captured and evaluated using a risk assessment of the potential resulting impact. Additionally, the assumptions relating to applicable compliance requirements should be considered.

FRAMEWORK ROLE ASSIGNMENTS

When the framework is applied within the organization, the assignments of various roles related to the ongoing management of the framework will be distributed among different groups. Assignments may include who is responsible for governance decisions pertaining to applicability or de-selection of the framework element, who is responsible for establishing the requirements and detailed specifications for the framework element, who is responsible for the delivery or execution of processes related to the framework functions, and who is responsible for oversight, monitoring, and measurement of the framework element performance.

FRAMEWORK ROLES

- Governance
- Requirements
- Execution
- Oversight

STANDARD RACI METHOD

- **R**esponsible - the person or group who is assigned to do the work

- **A**ccountable - the person or group who makes the final decision and has ultimate ownership
- **C**onsulted - the person or group who must be consulted before a decision or action is taken
- **I**nformed - the person or group who must be informed that a decision or action has been taken

As the framework is implemented, the role assignments should be captured across each element or control and tracked across the organization. Larger organizations may have numerous assignments based on divisions, business units, or other sub-organizational division factors. Additionally, outsourced solutions and Cloud Computing will introduce further role assignment factors.

FRAMEWORK ASSESSMENT

There are a number of criteria to consider during the implementation phases of the framework as well as the ongoing management of the framework elements and controls. A maturity model should be considered for the stages of implementation. Models can include:

Model	Capability Maturity Model (CMM)	Texas Cybersecurity Framework	NIST / C3 Cybersecurity for Critical Infrastructure	National Cyber Security Review (NCSR)
Level 0		Nonexistent		
Level 1	Initial	Ad-hoc / Initial	Tier 1 – Partial	Ad-Hoc (AH)
Level 2	Repeatable	Consistent / Managed / Repeatable	Tier 2 – Risk Informed	Documented Policy (DP) Or Documented Standards and Procedures (DSP)
Level 3	Defined	Compliant / Defined	Tier 3 – Repeatable	Risk Measured (RM) Or Risk Treated (RT) Or Risk Validated (RV)
Level 4	Managed	Risk-Based / Managed	Tier 4 – Adaptive	

Level 5	Optimizing	Efficient / Optimized / Economized		

CONSIDERATIONS

- Framework selection, scope, and prioritization decisions derived from Framework Assessment are outputs from the Information Security Strategy including short, mid, and long term planning
- Defining the effectiveness of the framework elements and controls in the Measurement and Metrics area of the Guide
- Defining the high-level role functions within the Governance and Organization area of the Guide
- Constructing a decision tree / flow diagram for specific framework selections
- Including a decision risk assessment template within the Information Security Risk Management area of the Guide

RESOURCES

The following resources are available to support the framework assessment process:

- Carnegie Melon Capability Maturity Model - http://www.sei.cmu.edu/reports/93tr024.pdf
- Texas Cybersecurity Framework - https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/AgencySecurityPlanInstructions.docx
- NIST / C3 Cybersecurity for Critical Infrastructure - http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

The following resources are available to support the framework selection process:

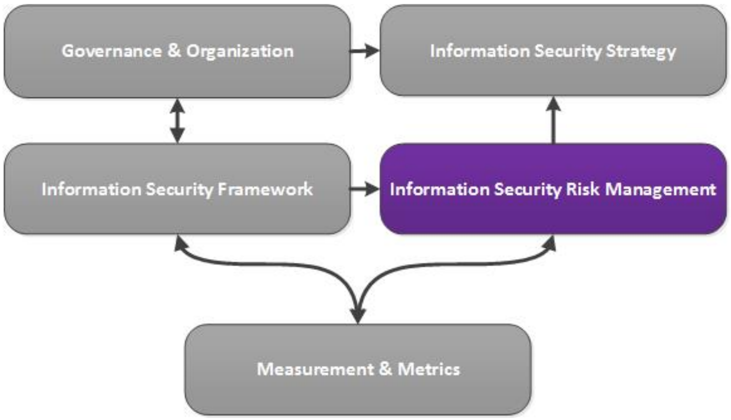
- Industry Standard Framework Crosswalk (Referenced to NIST800-53 Rev 4) - https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/DIR_Control_Crosswalk.xls
- NIST Special Publication Series 800 - http://csrc.nist.gov/publications/PubsSPs.html

The following resources are available to support the scope of framework application process:

- Industry Standard Framework Crosswalk to Various Compliance Requirements (Referenced to NIST SP 800-53 Rev 4) - https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/DIR_Control_Crosswalk.xls

INFORMATION SECURITY RISK MANAGEMENT

OVERVIEW


Governance & Organization
Information Security Strategy
Information Security Framework
Information Security Risk Management
Measurement & Metrics

An Information Security Risk Management process can be the centerpiece of an Information Security Program as it is the mechanism by which all other Program initiatives can gain visibility and business management support.

A well-executed process can help information security professionals, and those tasked with management of information security programs, define and understand the organization's risk tolerance levels while ensuring that executive management is kept aware and acknowledges responsibility for the security of the business.

AUDIENCE

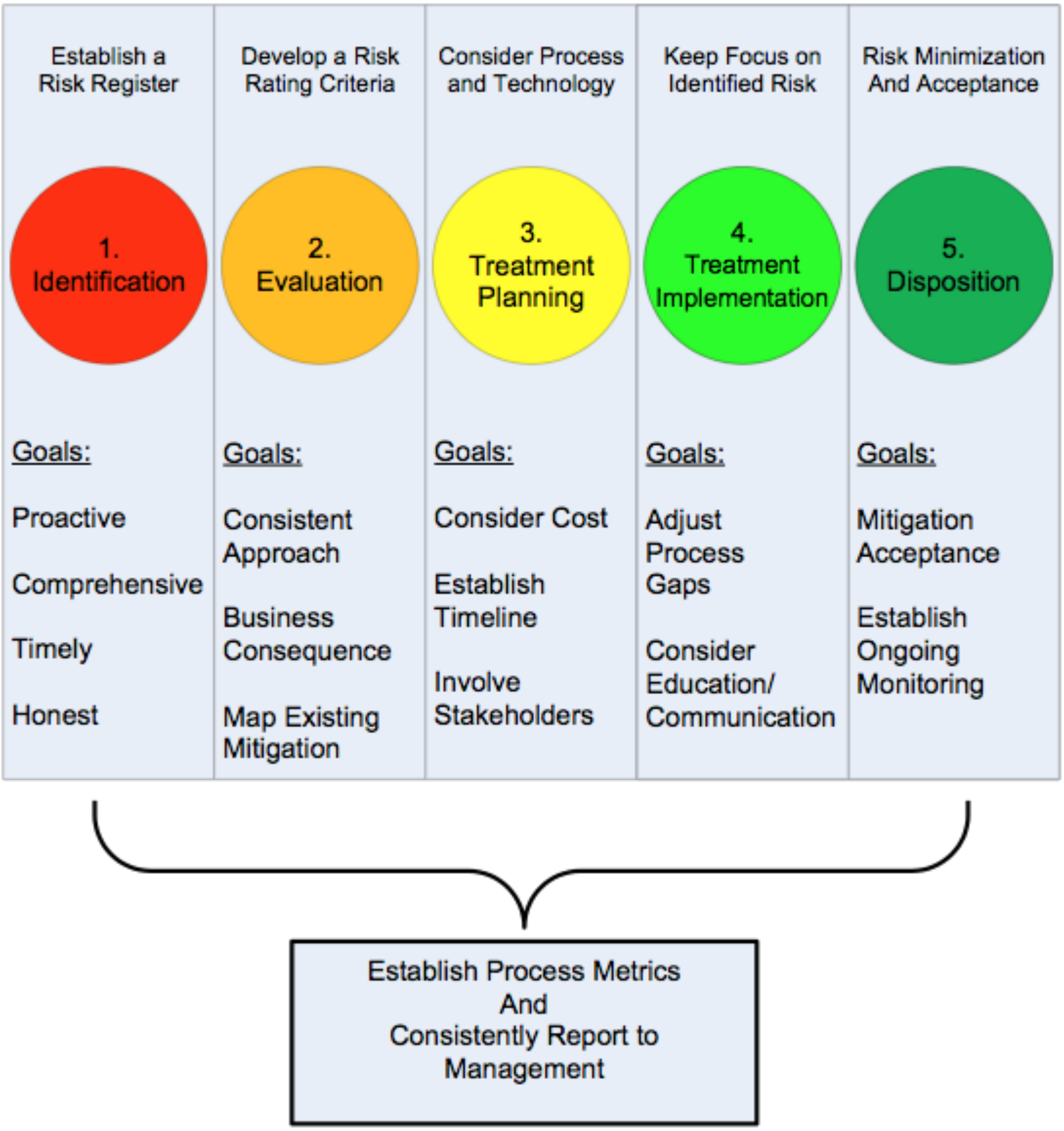
The primary audience for an Information Security Risk Management process should be the organization's executive leadership team. Due to their overall responsibility to the organization, they must understand and weigh in on major risk management decisions.

> The Information Security team is responsible for shedding light on the major risks that could disrupt the organization.

This team has the responsibility to ensure the process is adhered to and documented. A key responsibility for the Information Security team is to assist in translating IT and technical jargon into clear, concise language that can be understood by non-IT executives. The third audience group for an Information Security Risk Management process is variable based on the risk identified. All facets of the organization that handle, process or support key business areas must be made available to support the Information Security team and the risk management process.

COMPONENTS

The Five-Step Risk Management Process Components:



Establish a Risk Register	Develop a Risk Rating Criteria	Consider Process and Technology	Keep Focus on Identified Risk	Risk Minimization And Acceptance
1. Identification	2. Evaluation	3. Treatment Planning	4. Treatment Implementation	5. Disposition
Goals:	Goals:	Goals:	Goals:	Goals:
Proactive Comprehensive Timely Honest	Consistent Approach Business Consequence Map Existing Mitigation	Consider Cost Establish Timeline Involve Stakeholders	Adjust Process Gaps Consider Education/ Communication	Mitigation Acceptance Establish Ongoing Monitoring

Establish Process Metrics
And
Consistently Report to
Management

IDENTIFICATION

Risks can be identified via many sources:

- Program gap assessments
- Security operational metrics (e.g. patching, vulnerabilities)
- Audit findings
- New project/initiative risk assessments
- Compliance gaps
- Daily news (i.e. major security breaches or vulnerabilities)

- Industry associations (e.g. Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), or The National Council of Information Sharing and Analysis Centers)

Ideally, an organization will have structured risk assessment and operational security processes that can assist in defining new risks. The goal is to be proactive in identifying risks and to commit to documenting risks in a spreadsheet or database known as a risk register, while being comprehensive and honest.

> A mature Information Security Program is transparent, no longer hiding business critical risks within IT.

EVALUATION

The risk evaluation process can be a complicated matter, but generally, there are two options: quantitative and qualitative.

The *quantitative* approach seeks to define possible dollar loss due to the risk, considering reputational loss, data record costs, and availability loss. Although this is an effective method for gaining business buy-in, historically the quantitative approach has been perceived to require extensive information regarding the value of the assets, processes and information, as well as sparking debates regarding the methodology used to determine a risk-based dollar amount.

The *qualitative* approach is more widely used and can be considered an instinctual process by which risk probability and risk impact are evaluated. The challenge to this approach is to remain consistent and use established criteria for risk rating determination. Ideally, a group or committee that has experience in IT will complete this risk evaluation process.

Regardless of the risk evaluation approach selected, it is essential to map the identified risk to the business system or process that would be impacted. Another key element is to have clarity to the existing controls that serve to mitigate the new risk, even if not completely effective.

TREATMENT PLANNING

The Treatment Planning phase must include all of the stakeholders involved in the risk and business process affected. A balance must be reached in regards to risk mitigation options for both resource and control costs. An additional consideration in the Treatment Planning phase should include possible risk transference via contracted services or cyber insurance options.

Including the business owners will help clarify acceptable risk treatment plans. A key piece of treatment planning is to establish an acceptable timeframe for the remaining risk process steps. Again, having the stakeholders participate is critical to this decision making process.

TREATMENT IMPLEMENTATION

The Treatment Implementation phase must keep true to resolving the identified risk and enacting the treatment planning decisions established. Important elements of this phase include process evaluation and adjustments, not just the application of new technology. Considerations should include updating or creating new employee training and communication mechanisms.

DISPOSITION

The final phase of a risk management process is disposition, in which risk remediation has been validated as successful and the remaining residual risk can be accepted by all of the stakeholders. A key consideration of this phase is the establishment of risk monitoring processes that seek to ensure this specific risk is sufficiently resolved over time.

A recommended final step is to review the documentation elements that map the risk from Identification to Disposition, providing clarity to auditors and regulators who might need to revisit your organization's effort in managing risks. This final risk management step must also include the reporting of risk management activities to the appropriate oversight group to ensure risk tolerances are in-line and acceptable by the corporate leadership team.

CONSIDERATIONS

> The success of your risk management process begins with establishing business leaders and executive management oversight of the process.

They must be directly involved in reviewing the process output and must have visibility to the efforts produced by the Information Security team and risk stakeholders.

If managed correctly, Information Security leaders will enable the business to focus resources on the most significant risks to the organization while making sure executive management is kept responsible for the actions and inactions of the organization's teams. In order to do this effectively, risk management process metrics must be defined, easy to understand, and consistently reported to the business leaders and executive management oversight committee.

RESOURCES

Risk Register Overview - http://en.wikipedia.org/wiki/Risk_register

Open Source Information Security Risk Register Tool - http://www.iso27001security.com/ISO27k_Risk_Register_v2.xlsm

NIST Special Publication 800-30 *Guide for Conducting Risk Assessments* - http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

The Failure of Risk Management: Why It's Broken and How to Fix It, by Douglas Hubbard, Wiley, 2009

How to Measure Anything: Finding the Value of Intangibles in Business, by Douglas Hubbard, Wiley; 3rd edition 2014

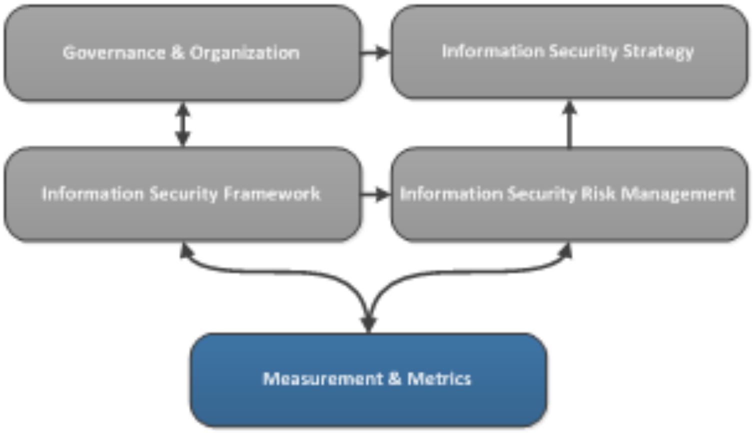
Factor Analysis of Information Risk - http://en.wikipedia.org/wiki/Factor_analysis_of_information_risk

The Society of Information Risk Analysts (SIRA) - http://www.societyinforisk.org/

Assessing Information Security Risk Using the OCTAVE Approach - http://www.cert.org/resilience/products-services/octave/

MEASUREMENT AND METRICS

OVERVIEW


Governance & Organization
Information Security Strategy
Information Security Framework
Information Security Risk Management
Measurement & Metrics

An important part of an effective information security program is the ability to measure the current operational and security status of an organization and to maintain situational awareness of activity. Key to this ability are the metrics that will be used to determine what should be monitored, what data should be collected, and what historical organizational figures are needed in order to be able to measure them against the current state of the organization and its information resources. It is important to note that there are traditionally three reasons to gather and report metrics:

- Compliance requirements (e.g. external regulatory requirements for a given sector);
- To be able to "tell the story" about the current security status of the organization that you want to be able to convey to senior management; and
- To gather appropriate information necessary to make decisions about the organization's security program (e.g. trends, work to accomplish, recommendations, strategic direction, etc.).

It is important to note that while the temptation might be to monitor, gather data, and report on the numbers obtained, a good metrics program goes farther. Simply reporting various numbers may not immediately indicate what the issues are or the ramifications of those numbers. Data needs to be tied to specific organizational goals and objectives – especially security objectives.

A good metric will be more than just a number; it will be an indicator of how well an objective is being met.

Metrics should also be provided over time so that trends, either positive or negative, can be more easily noted.

An additional benefit of a good metrics program should not be overlooked. The measuring and reporting on various aspects of an organization's security program will also help to make leaders more aware of security issues in general. As awareness grows, it will become easier for security professionals to obtain support for security initiatives, as leaders will better understand how a lack of security can impact the organization.

AUDIENCE

Metrics should be used to provide a picture of the current security status to different audiences within the organization. Each of these audiences may need a different metric, or at the very least, a different method to display or explain the metric, for it to be useful. The list of possible audiences include:

- Business Leaders and Executives
- Enterprise Risk Committee
- Information Security Personnel and Direct Reports to the Information Security Program owner (i.e. the Chief Information Security Officer, Security Director, or other designated person)
- CIO and IT Personnel

When considering security metrics for business leaders, the most important question is: What information on security do they want in order to better make decisions for the organization? Too often security professionals will want to display minute details about the technology or "inner workings" of the network that are inappropriate for an executive audience. This is especially true when a metrics program is launched. The goal should be to keep the categories of information provided to a minimum so that it can be more easily understood. As the comfort level and understanding of business leaders grows, they will be better prepared to understand additional details, and in fact may request more details once they have become aware of the potential damage that could happen to the organization should a security incident occur.

An additional approach for an executive audience, including the Enterprise Risk Committee, is to provide data grouped into categories of business interest. These categories might include financial (e.g. how much are you spending on security), business enablement (e.g. the level of impact on business as a result of various security issues), compliance (e.g. status of controls within specific business units), and awareness (e.g. how well internal training efforts are positively affecting employee behavior).

> IT management is concerned with those issues that will impact the traditional concerns of confidentiality, integrity, and availability of applications, data, and resources.

IT management is concerned with the daily operations of the technology infrastructure, so metrics for these individuals will be more technical in nature. They will want to know about those issues that will impact the traditional concerns of confidentiality, integrity, and availability of applications, data, and resources. Indicators that any of these may be at risk will be of significant interest to an IT audience.

Security professionals, and those tasked with information security management, will be interested in even more detailed technical information as it relates to security. Updates to signatures for intrusion detection/prevention (IDS/IPS) systems or firewalls, daily numbers and types of attacks/probes, number/rate of failed logins, software defect counts, average time to remediate security issues, and similar numbers may all be of interest to this audience.

For all audiences, attempt to distill the information to a level that is appropriate for the intended recipients.

COMPONENTS

Components of a metrics program will vary, and no list exists that will completely or accurately describe the metrics that every organization would need to consider. Instead, from a general perspective, your metrics program should include a description of:

- The methods your program uses to record, track, and report key performance indicators
- The methods your program uses to record, track, and report key risk indicators
- Your use of metrics in support of a continual improvement process for the program

There are a plethora of possible things to measure to provide a real-time picture of the current security status of an organization. We provide here just a sampling of different metrics that might be used. This list is by no means definitive nor is it complete. What any specific organization will use to present a picture of their current status depends heavily on the type of organization, its potential threats, and the desires of management. The items listed here are for illustrative purposes only, in order to help provide a better understanding of the variety of metrics that can be utilized.

BASELINE DEFENSES COVERAGE

"This is a measurement of how well you are protecting your enterprise against the most basic information security threats. Your coverage of devices by these security tools should be in the range of 94 percent to 98 percent. Less than 90 percent coverage may be cause for concern. You can repeat the network scan at regular intervals to see if coverage is slipping or holding steady. If in one quarter you've got 96 percent antivirus coverage, and it's 91 percent two quarters later, you may need more formalized protocols for introducing devices to the network or a better way to introduce defenses to devices." [3]

PATCH LATENCY

"Patch latency is the time between a patch's release and your successful deployment of that patch. This is an indicator of a company's patching discipline and ability to react to exploits. As with basic coverage metrics, patch latency stats may show machines with lots of missing patches or machines with outdated patches, which might point to the need for centralized patch management or process improvements." [3]

LEGITIMATE E-MAIL TRAFFIC ANALYSIS

"Legitimate e-mail traffic analysis is a family of metrics including incoming and outgoing traffic volume, incoming and outgoing traffic size, and traffic flow between your company and others.

There are any number of ways to parse this data; mapping the communication flow between your company and your competitors may alert you to an employee divulging intellectual property, for example." [3]

CONSIDERATIONS

As stated earlier, the metrics provided to various individuals in the organization need to be tailored for those individuals and should provide what they want and need to know to make decisions at their level. It will be important to provide information on a regular basis. A schedule for reporting should be developed so that reports can be provided at times when they can best be used for decision-making within the organization.

For business leaders and executives, the type of metrics that might prove useful could include overall program metrics such as total risks, risk remediation metrics, exception to policy, and incident metrics. IT management, on the other hand, will have a more keen interest in the actual day-to-day operations of computer systems and networks and metrics for this audience will generally be more technical in nature and might include server, workstation, database patching, and vulnerability metrics.

The use of metrics to provide a picture of the status of security ultimately is for the purpose of helping the organization secure their various assets. That said, there may be a temptation to provide reports and data that indicate where individuals or part of the organization have failed. This should be done with extreme caution. The goal is not to alienate any part of the organization but instead to garner support for the security program. New metrics should not be introduced without some advance preparation with those who will need to understand it and those who may be impacted by it. Using metrics as a hammer should only be done as a last resort when nothing else has worked to get the attention of those responsible. Generally, it is better to work with those for which the metrics might indicate a problem so that you are viewed as supporting them and not trying to advance your own agenda or career.

It might also be tempting to report numbers for things that to a security professional may seem important or interesting, but to an executive or business leader may not. If you have no influence over the metric, or there is not action that you are going to recommend as a result of this metric, consider not reporting it. For example, the number of attacks detected by the IPS is interesting and should be tracked, but if you aren't going to recommend anything as a result of that number, then don't include it in regular reporting outside of the security organization. If, on the other hand, you have noticed a twenty-fold increase in attacks aimed at a specific port or service, this might be an indication of something and you may want to make your leaders aware of this increase and what you are recommending be done as a result. This may especially be true if it is related to a vulnerability that has been recently been reported in the media about which your leaders may have heard.

Data, both good and bad, should be reported so that potential problems can be identified.

As a final note, the temptation may exist, especially for a new program, to only report on those items that indicate a problem may exist. Data, both good and bad, should be reported so that potential problems can be identified, but also so that successes can be noted to ensure that leaders know that previous efforts have had the desired impact. At the same time, it is important to note that complacency can also be detrimental to a metrics program as numbers that are reported regularly without change or an understanding of their significance will eventually be ignored. If a metric is being used to support a decision then it should be reported. If it's not of interest, then it should stop being reported.

Reporting metrics is an opportunity to market and promote the Information Security Program. Use it to demonstrate how the program has grown and matured and how the organization's investment in security is working for its protection.

RESOURCES

[1] Security Metrics: Replacing Fear, Uncertainty, and Doubt, by Andrew Jaquith, Addison-Wesley, 2007.

[2] *A Guide to Security Metrics*, SANS Institute INFOSEC Reading Room, 2006, http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

[3] *A Few Good Information Security Metrics*, CSO Online, 2005, http://www.csoonline.com/article/2118152/metrics-budgets/a-few-good-information-security-metrics.html

[4] *Establishing a Security Metrics Program*, SANS Technology Institute, Final Project Report, www.sans.edu/student-files/projects/jwp-caincouture-whitepaper.doc

[5] *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*, by Lance Hayden, McGraw-Hill, 2010

[6] *Security Metrics, A Beginner's Guide*, by Caroline Wong, McGraw-Hill, 2011

[7] *How to Measure Anything: Finding the Value of Intangibles in Business*, by Douglas Hubbard, Wiley; 3rd edition 2014

[8] *The Failure of Risk Management: Why It's Broken and How to Fix It*, by Douglas Hubbard, Wiley, 2009

GLOSSARY

The following terms are commonly used with regard to information security:

Attack - Various technical and process-based actions designed to identify and overcome an organization's defenses. Examples include web-based attacks (e.g. Cross Site Scripting, Buffer Overflow, SQL Injection), network-based attacks (e.g. teardrop, denial of service) or physical attacks (e.g. social engineering, attempts to enter restricted areas).

Control – A countermeasure that would reduce or mitigate risks posed to an organization's resources, personnel, business relationships, or reputation.

Cyber Extortion – Attempts by external or internal parties to extract remuneration from an organization based on threats to disclose sensitive information or render the organization's assets ineffective. May include denial of service attacks against a web property or data network.

Defacement – Unauthorized modification of data on web sites intended to discredit the web site's owner or present a message or platform for social or political purposes.

Disgruntled Insider - Includes current and former employees, contractors, or vendors with access to the organization's data and systems.

Firewall - A technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts.

Governance and Organization - Governance and Organization is a structure around how organizations align security strategy with business strategy, and implementing methods to manage the performance and continual improvement of the organization responsible for information security operations.

Hacktivist - Attackers primarily motivated by social or political goals (e.g. Anonymous, the Syrian Electronic Army, or various privacy rights groups).

Information Security Framework - An Information Security Framework is a selection and implementation of a set of security program components generally recognized by industry and business partners. Frameworks are used for assessing the effectiveness of security controls.

Information Security Steering Committee – A body composed of subject matter specialists and designated members of an organization's management charged with overseeing the information security function of the organization. Depending on the Committee's charter, may be charged with analyzing and considering identified risks, accepting those risks, or recommending to senior management whether risks should be remediated or accepted. The Committee may also be used to provide direction and oversight to the organization's information security team.

Information Sharing and Analysis Centers (ISACs) - Operated by the National Council of ISACs, these industry bodies are organized specific to various industries and designed for information sharing between organizations.

Information Security Strategy - Information Security Strategy is a formal, high-level, communicated plan approved by executive management that asserts how the organization intends to treat and protect business sensitive information. The strategy aligns to the organization's business objectives.

Measurement and Metrics - Measurement and metrics are the methods used to record, track, and report key performance indicators. Metrics support a continual improvement process for security.

Nation States - Countries that perform bulk data collection using cyber intelligence and cyber-attack methods. These countries collect data for future analysis and target a broad range of government and commercial organizations including emerging technology companies.

Penetration Test - Use of a combination of automated tools and manual processes to attempt to actually exploit vulnerabilities in systems or processes.

Risk - The potential of losing something of value. The intentional interaction with uncertainty.

Risk Register - A central repository for all risks identified by an organization and, for each risk, includes information such as risk probability, impact, controls (counter-measures), risk owner, etc. May also be used to record risk acceptance decisions by an approved member of management.

Risk, Threat, and Vulnerability Remediation - Risk, threat, and vulnerability remediation is the set of actions implemented to reduce, transfer, or eliminate factors that can actually or potentially impact information and information systems in an adverse manner.

Security Professional - An individual who performs security tasks for a majority of his/her time. He/she may have received specialized information security training or possess one or more recognized security industry professional certifications.

Security Risk Management - Security Risk Management consists of processes and procedures to continually identify, analyze, consider, and treat risks based on business context and the risk appetite of the organization.

Social Engineering - Efforts to obtain confidential information by manipulating and/or deceiving people. Common vectors include telephone calls, specially crafted e-mails or malicious web sites.

Threat – An indication or warning of a condition that would cause harm to an organization’s resources, personnel, business relationships, or reputation.

Vendors - An external individual or company that provides products or services to your organization. Vendors that provide certain security services may be known as Managed Security Services Providers (MSSP).

Vulnerability - A weakness in technology or process that may be exploited to negatively impact the confidentiality, integrity, or availability of data.

Vulnerability Scan - A process to use automated tools augmented by manual processes to identify the existence of vulnerabilities in a system or network.

LICENSE