ESSENTIAL FUNCTIONS OF A CYBERSECURITY PROGRAM

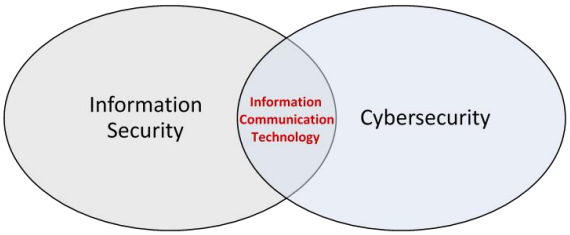
Introduction

No matter the size of an organization, every organization that depends on *information technology* to conduct any part of its business should have a functioning *cybersecurity program*.

Over the last several years as dependence on IT and Internet connectivity have grown, many businesses have under recognized their *cyber footprint*. The term "Cyber footprint" describes the relationship between *information* and the associated layers of people, processes, and technology necessary to assure the business purpose of that information. An organization's cyber footprint may be as simple as a single computer containing business records or as complex as a multi-endpoint local area network supported by cloud solutions. In either case, cybersecurity begins with protecting information and extends through the layers of infrastructure supporting its use.

In offering some context, terms surrounding the ***protection of information*** and ***information resources*** have evolved over time as new technology and concepts have come into use in the business mainstream. The evolution of these terms should be thought of as inter-linking parts of the bigger business risk model.

Information Security is just that, protection of information whether in electronic or physical form. *Cybersecurity*[1] incorporates that definition to include electronic delivery of information by means of Information Communication Technology (ICT).[2]



> "Cybersecurity has quickly evolved from a technical discipline to a strategic concept. Globalization and the Internet have given individuals, organizations, and nations incredible new power, based on constantly developing networking technology. For everyone – students, soldiers, spies, propagandists, hackers, and terrorists – information gathering, communications, fund-raising, and public relations have been digitized and revolutionized.
>
> …

1 U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#C (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009).

2 Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. [ISO/IEC 2382] (adapted

> In cyber conflict, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbor in cyberspace. Hardware, software, and bandwidth form the landscape, not mountains, valleys, or waterways. The most powerful weapons are not based on strength, but logic and innovation."[3]

No matter the specific 'security' term used, the objective remains to assure:

Confidentiality – "the circumstance whereby data or information is *not* made available or disclosed to unauthorized persons or processes"

Integrity – "the circumstance whereby data or information have not been altered or destroyed in an unauthorized manner"

Availability – "the circumstance whereby data or information is accessible and useable upon demand by an authorized person"

*Throughout this document the term Cybersecurity will be used to include all facets of information protection.

What is a Cybersecurity Program?

Today's business landscape is defined by the *people*, *processes*, and *technology* used to manage its *information*. That information is *the* essential element for most businesses. Therefore, it stands to reason that the only approach for sustainable cybersecurity is to involve the business' people, process, and technology in the solution. This means that cybersecurity should be perceived as an enterprise-wide undertaking, a corporate discipline, not an IT project. As such, cybersecurity should be viewed as a full-fledged business program within the organization's functional business structure. [4]

A *program* approach to Cybersecurity:

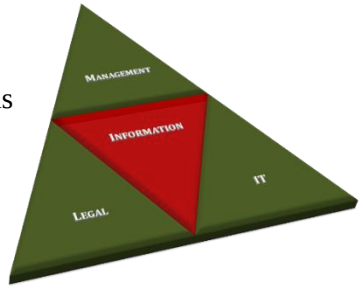
- Provides the structure and processes essential to control cybersecurity operations and react to evolving changes to information risk.
- Supports the business' vision, goals and objectives. Business allocation of resources influences the cost and success of the program from an enterprise perspective, not as a part of IT budget.
- Integrates component parts necessary to power the intended whole. Allows for continual performance optimization functionally and technically.
- Assures adherence to standards and alignment with the business vision. Also, facilitates accountability and management of component projects. Tracks basic component costs together with wider costs of administering the program.

[3] Strategic Cybersecurity, Kenneth Geers, NATO Cooperative Cyber Defence Centre of Excellence, June 2011

[4] A plan of action aimed at accomplishing a clear business objective, with details on what work is to be done, by whom, when, and what means or resources will be used.; Programs deliver outcomes but projects deliver outputs

Cybersecurity is not a *project* because:

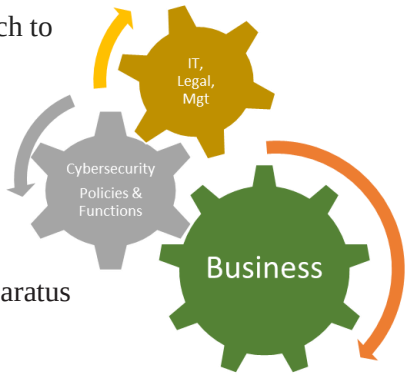
- A project is unique, discrete and of definite duration. A program is ongoing and chartered to consistently achieve certain enterprise level results.
- A project is designed to deliver an output or deliverable; project success is judged on delivering the right output at the right time and cost.
- A program's success will be measured in terms of benefits.
- Programs are capable of reacting to changes in strategy and environment as the organization changes.



In most businesses, the need, use, and protection of information is bounded by three functional areas —business management, legal considerations (regulations and contractual arrangements), and the use of Information Technology to support the whole. Business goals change, new legal requirements around how information should be used and protected emerge, and new technology is regularly adopted in support of those changes. So, while implementing effective people, process, and technology controls is essential to protecting information, anticipating change around business need and use of information should be an equal consideration.

With those thoughts in mind, a Cybersecurity Program should be viewed as an over-arching, enterprise-wide sequence of constantly expanding and contracting activities. These activities are *Prevention*, *Detection*, and *Response*.

- *Prevention* activities may include security architecture design, security awareness and training, and policy development for example. Any activity that will limit or contain a potentially damaging cybersecurity event.
- *Detection* activities may include system log analysis, visitor log analysis, event reporting by users for example. These are activities that enable discovery of cybersecurity events.
- *Response* activities are action steps involving resources and communications necessary to contain the threat and recover business operations. *Response* activities may span from analysis of anomalous but non-threatening events to incidents to data breach to a crisis.



For that reason, it is essential that the Cybersecurity Program be orchestrated and *synchronized* with the organization's business goals and be inherently flexible enough to realize real world risk and compliance issues at the same time. Achieving this 'synchronization' is foremost a matter of adopting an inclusive information management controls framework and building a working program apparatus

based on **that** framework. In doing so, every business can begin to recognize information risk and start managing that risk in a systematic way.

Information Protection Frameworks, Standards, and Regulations

There are multiple frameworks for managing information risk. Each organization is different, and the applicable framework may be predetermined for the organization by regulation. Or, the best framework may be a compilation of frameworks and best practice components cobbled together to create a custom framework unique for the organization. In addition to the previously mentioned NIST Cybersecurity Framework,[5] the International Organization for Standardization (ISO) has issued the 27000 series of standards. ISACA has issued the Control Objectives for Information and Related Technology (COBIT) Framework. The authors of this document do not recommend the use of one standard or framework over others. Each of these standards and frameworks contain elements that may be helpful to companies managing their information security risk.

ISO/IEC 17799:2005 defines guidelines and general principles for initiating, implementing, maintaining, and improving information security management within any organization. The specified controls provide recommendations involving:

[5] http://www.nist.gov/cyberframework/upload/ cybersecurity-framework-021214.pdf

- SECURITY POLICY
- ORGANIZATION OF INFORMATION SECURITY
- ASSET MANAGEMENT
- HUMAN RESOURCES SECURITY
- PHYSICAL AND ENVIRONMENTAL SECURITY
- COMMUNICATIONS AND OPERATIONS MANAGEMENT
- ACCESS CONTROL
- INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE
- INFORMATION SECURITY INCIDENT MANAGEMENT
- BUSINESS CONTINUITY MANAGEMENT
- COMPLIANCE

Cybersecurity Program Functions

> "Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly."
>
> —IT Governance Institute, Board Briefing on IT Governance, 2nd Edition, USA, 2003

Obviously, Cybersecurity Governance is the center piece from which each of the activities previously described, *Prevention—Detection—Response*, must be coordinated. But, because critical information is so pervasive in most organizations, there are other important functions that must include cybersecurity considerations. In addition to core Cybersecurity Operations, those functions are:

- Planning
- Project Support
- Risk Management

Governance

Although businesses often try to relegate privacy and information protection responsibilities to an IT management function, all parts of the organization must accept ownership responsibilities for information protection. The reasoning is simple. Within each organization there are functions that *own* information,

functions that are *custodians* of information, and there are *users* of information. For example, an employee database may be managed by IT, but they are merely the *custodians* of the information within that database. Similarly, line managers may use the database to perform a variety of functions but they are simply *users* of the information. Does HR *own* the database?

The board of directors, management, and internal auditors all have significant roles with information protection controls.

- The board of directors must provide program oversight of information ownership, protection, policies, and shaping corporate culture to enable information protection.

- Executive management must provide leadership to ensure that information protection efforts are supported and understood across the organization, this includes dedicating sufficient resources for information management controls to be effective. Executive management must review activities for continuous improvement and ultimately be responsible for the success of any information protection project.

- Staff and line managers must be integrated in the design and implementation of all information protection activities, especially information resource classification (sensitivity and/or criticality). Likewise, they must review and monitor operation of information protection controls to ensure appropriateness, in spite of changing risk and business requirements.

- Every business must create, communicate, and enforce well-defined policies and procedures that reflect a consensus of risk management decisions. Policies can only be enforced if they are up-to-date, relevant to the business, and communicated appropriately. Policies and procedures are the road-maps by which the organization should be using, moving, and storing information.

- A Cybersecurity leadership role must be created. That role should be *empowered* to coordinate, manage, recommend and escalate all issues regarding business information risk. This executive must have access to all resources necessary in order to interpret applicable laws and regulations that govern how the business controls sensitive information, as well as advise the board and senior management on what the organization perspective should be regarding various information risk issues.

1) Operations

Prevention of Threatening Events

Creating, implementing, and oversight of safeguards intended to ensure delivery of critical information and services for the business.

These activities typically include:

- Establishing an ***Information Security Architecture*** consistent with the organization's Cybersecurity Governance directions, necessary to protect the confidentiality, integrity, and availability of information

- User and Staff ***Security Awareness and Training*** including role based and privileged user training

- Defining and implementing ***Information Protection Processes and Procedures*** necessary to maintain and manage information resources

- ***Identity Management and Access Control*** for the organization, including physical, digital, and remote access

Detection of Threatening Events

Activities that enable the timely discovery of cybersecurity events.

These activities typically include:

- Defining and implementing ***Continuous Security Monitoring*** capabilities to monitor for cybersecurity events

- Develop and implement ***Detection Processes*** to warn of anomalous events

- ***Vulnerability Management*** conduct vulnerability scans routinely to assess system vulnerabilities and coordinate with IT management on remediation. Conduct "red team" tests and coordinate with Infrastructure management accordingly.

- ***Cyber Investigations*** analyze cyber events to help determine cause and effect

Response to Threatening Events

Actions regarding potentially damaging or threatening cybersecurity events. Where the impact of a potential cybersecurity incident is determined, execute the appropriate Cybersecurity Incident Response Plan.

These activities are directly tied to these definitions:

> ***Event*** —An event is any observable system or network situation, condition, or activity. Adverse events involve negative consequences, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
>
> ***Incident*** —An incident is the culmination of an event or events leading to a judgement that the confidentiality, integrity, or availability of sensitive or critical information or associated

information systems may be subject to compromise (potential for breach). *Incident may describe both intrusions (from outside the organization) and misuse (from within the organization).

Breach —Definitive loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access of sensitive or critical information.

Cyber Crisis — An *abnormal situation* that threatens that organization's **objectives**, **reputation**, or **viability**. These events involve the organization's ability to assure the *confidentiality*, *integrity*, or *availability* of certain *information* or *information resources* critical to the organization's operation. They may be defined as a breach, compromise or disruption of the organization's critical data or systems.

These activities typically include:

- ***Follow Response Planning*** protocols in accordance with defined level of threat
- ***Manage Communications*** during and after an event with stakeholders, law enforcement, third parties (vendors/clients/partners) as appropriate
- ***Analyze Events*** to ensure effective response and support recovery activities including forensic examinations, and facilitate determination of the impact to the organization
- ***Immediate Mitigation*** to prevent expansion of an event and to resolve the incident
- ***Recover*** assistance for timely recovery to normal operations impact reduction
- ***Identifying Improvements*** based on lessons learned and reviews of existing policies, procedures, guidelines, and activities

2) Planning

Activities supporting all aspects of the cybersecurity functions.

These activities typically include:

- ***Research new technology*** and process changes for potential vulnerabilities
- Creating and maintaining a ***Knowledge Management*** function that collects and maintains information that is relevant to the information security program. This may include details about the cybersecurity program as well as background on threats, vulnerabilities, tools and templates used to implement the program.
- Assist in ***drafting and implementing Cybersecurity Policy and Procedures***

3) Project Support

These activities typically include:

- ***Cyber Risk Guidance*** on all projects undertaken by the organization
- ***Clarifying Implementation Questions*** consistent with the information security policy and the organizational risk tolerance

4) Risk Management

These activities typically include:

Risk management is the ongoing process of balancing business opportunity with the impact of threats exploiting vulnerabilities. The Risk Management function is the engine that drives the program. The Risk Management function leverages industry best practices and standards as well as best of breed tools to determine the value at risk for the business and thus the level of resourcing appropriate for mitigation efforts. The risk assessments are continuously updated, monitored, and tracked with input from the other components.

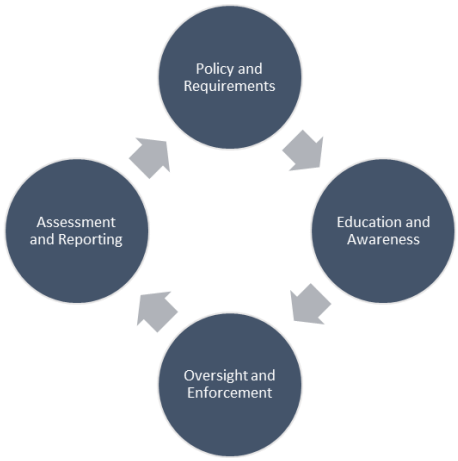
- Conduct routine ***Internal Information Risk Assessments***
- Conduct ***Third-Party Vendor Information Risk Assessments***
- Identify specific regulatory requirements such as PCI, HIPAA, SOC2, ISO 27001, DFARS, etc., and define conformity Identify
- Identifying a ***Supply Chain Risk Management*** strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks

These functions describe those activities necessary to provide basic cybersecurity coverage. In larger organizations each function may represent a separate team. In some organization any or all of these functions may be outsourced. There is no direct correlation between size of a business and the size of its cybersecurity program, the basic functions will always be the same.

Managing the Cybersecurity Program Life Cycle

An information security program is never static. There will always be areas for improvement, new vulnerabilities to correct, policies to update, assessments to conduct, new technology to incorporate, etc. The Security Project Management component leverages the best practices in the areas of operational performance and project management to organize and manage the projects required to make the information security program function. This function develops the organization's project roadmaps to fill gaps, develops plans of action, develops and socializes business cases for projects, and performs project budgeting, monitoring and control. This component also supports resource management through an integrated master plan and schedule.

A Cybersecurity Program Life Cycle involves establishing **information security requirements**, **educating** people about their responsibilities, **building governance** structures to ensure compliance, while **monitoring and reporting** progress in order to **adjust policy** or requirements appropriately.



This approach should be perpetual. That is to say, based on conclusions derived from *security incident analysis* or *security compliance assessments* policy and/or procedure will be refined by these activities, *education* and *awareness* will be adjusted to better focus on current issues, and the cycle renews.

Managing Cybersecurity

Decision making is a cognitive process that defines a course of action to be taken in expectation of achieving a pre-defined result. In view of that, a decision cycle is the sequence of steps repeatedly employed to achieve those results while learning other potential outcomes and adjusting as needed.

Adaptive management is decision making in the face of uncertainty that relies on learning as an inherent part in order to achieve a best outcome based on current knowledge.

For example, each of these concepts are easily and routinely applied to IT management. Each rely on the idea that a metric will be produced based on outcome and there is a predetermined outcome envisioned. IT management is 'outcome driven'. Cybersecurity management is not.

While cybersecurity management should be expected to be integrated into those decision-making approaches as well, especially when a 'security project' is involved, cybersecurity management must live by a time-based decision-making concept too. Within Cybersecurity time becomes the one critical constant in all efforts. For example, the strength of encryption is ultimately based on time needed to break the code; the time to break into a safe is measured in 'torch and tool' time needed to penetrate its armor;

'dwell time' describes how long malware resided in a system prior to discovery and eradication, thereby estimating a compromise period. Cybersecurity is rarely static.

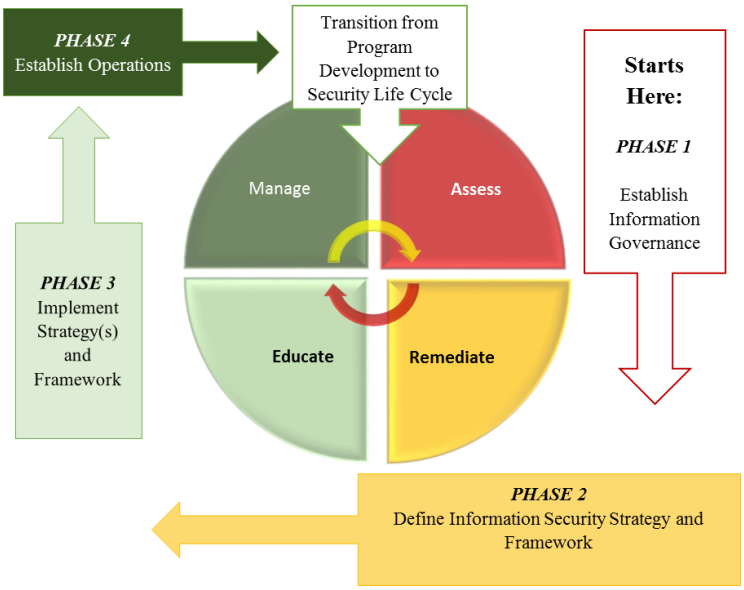
Management by OODA Loop

The concept of the OODA loop (observe, orient, decide, and act) was advanced as a military decision cycle in response to an event. [6] In its original context, the OODA loop was an air-to-air combat technique that led to reaching tactical solutions more quickly than one's opponent. The idea being, the pilot going through the cycle in the shortest time wins. Thus, the OODA loop introduces the concept that a manager that can respond to a threatening situation in the shortest time is more likely to be successful.

The OODA loop approach to cybersecurity equally takes into account the circumstances where the situation may change rapidly, meaning one threat and/or vulnerability must lose priority to another, as is often the situation in cybersecurity. Reaching a decision point about whether or not a breach has occurred should not be a rote effort.

Cybersecurity Program Development, The BorderHawk Method

The BorderHawk Method is a methodical management approach for establishing information security and Cybersecurity programs within existing organizational structures. Program development is based on four (4) sequential development *phases* anchored to particular *objectives* that are intended to be achieved through the completion of purposely designed *tasks*.



The process is designed to follow a sequential approach beginning with the recognition and establishment of the organization's *information owners*. The tasks are designed from the perspective of a security architect, presumably the organization's eventual *Information Security Advocate*.

The BorderHawk Method is:

[6] United States Air Force Colonel John Boyd

Phase I —Establish Governance

Objective: In accordance with applicable laws and regulations, create or adopt an information security framework (standard) that enhances the organization's business objectives, and then harmonize that framework with an information security strategy

Tasks:

1) Obtain senior leadership's commitment and support for information security across the enterprise.
2) Conduct Information Risk Assessment (IRA) using appropriate tool.
3) Create an Information Protection Council (IPC)
4) Adopt the organization's Information Security Program Charter
5) Appoint an Information Security advocate (CISO, CSO, etc.)
6) Define information security governance roles and responsibilities.
7) Define information security governance activities.
8) Define information security governance communication channels.
9) Create information security governance reporting processes and requirements.
10) Establish association with the organization's legal advisor in order to identify potential information security legal or regulatory issues across the enterprise.
11) Define an information security strategy in support of organizational purpose and strategy; ensure synchronization with information security framework.
12) Define an information security strategy in support of organizational purpose and strategy; ensure synchronization with information security framework.
13) Create and gain approval of an organizational Information Security Program Charter.
14) Identify internal and external resources (finances, people, and equipment) necessary to support the information security program and gain senior leadership approval.
15) Conduct end users impact analysis to establish information security policy requirements.
16) Create and gain approval of enterprise information security policies in accordance with accepted information security governance activities and the Information Security Program Charter.

Phase II —Define Information Security Strategy and Framework

Objective: Define the course(s) of action necessary to implement the strategy

Tasks:

1) Using conclusions from the IRA, gauge 'Expected Activity' to determine 'Program Maturity'.
2) Identify those functional activities necessary to accomplish the information security strategy and document same in an Information Security Program Manual; Ensure alignment between the information security program and all other organizational functions (physical, HR, quality, IT).
3) Develop information security architectures (people, processes, technology).
4) Plan projects necessary to implement the information security governance framework.
5) Design an information security awareness, training, and education program.
6) Socialize and integrate information security responsibilities into the organization's processes (change control, mergers, and acquisitions, etc.) and life cycle activities (development, employment, contracts, and procurement).
7) Develop information security risk management and compliance procedures.
8) Define metrics to evaluate information security program effectiveness.

Phase III —Implement Strategy(s) and Framework

Objective: Implement the information security strategy(s) and framework

Tasks:

1) Communicate information security policies that support the security strategy; Lead the development of procedures and guidelines that support approved information security policies.
2) Execute information security governance projects.
3) Collect information security in accordance with baseline data through information risk and vulnerability assessments.
4) Integrate information security program requirements into the organization's life cycle activities.
5) Promote accountability by business process owners and other stakeholders in managing information security risks.

Phase IV —*Operate*

Objective: Oversee and direct information security activities in accordance with IPC direction, adopted strategy(s), and framework

Tasks:

1) Manage all resources (finances, people, equipment, systems) dedicated to the information security program.
2) Monitor, measure, test, and report on the effectiveness and efficiency of information security controls, as well as compliance with information security policies.
3) Monitor information security controls in contracts (with joint ventures, outsourced providers, business partners, customers, third parties, etc.).
4) Deliver information security awareness, training, and education to all employees, contractors, or other third parties as might be appropriate, on a regular basis.
5) On both a periodic and event-driven basis, report risk changes to leadership in accordance with Information Security Program Charter; facilitate risk resolution in accordance with Information Security Governance directions.
6) Ensure that noncompliance issues and other variances are resolved in accordance with Information Security Governance directions, but always in a timely manner; mitigate risk to levels acceptable to the enterprise as directed.

The BorderHawk Method provides the initial step in developing an effective Cybersecurity program. As each task is accomplished, the effort should be moving toward an *operational security life cycle*.