Essential Functions of a Cybersecurity Program

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 has grown, many organizations have failed to recognize the extent of their cyberfootprint—that is, the relationship between information and the people, processes and technology necessary to assure the business purpose of that information. An organization's cyberfootprint may be as simple as a single computer containing business records or as complex as a multi-endpoint local area network (LAN) supported by cloud solutions. In either case, cybersecurity begins with protecting information and extends through all the layers of infrastructure supporting its use.

Terms related to the protection of information and information resources have evolved over time as new technology and new concepts have entered the business mainstream. These terms should be thought of as describing interconnected parts of the bigger business risk model (figure 1).

Information security is the protection of information, whether in electronic or physical form. Cybersecurity incorporates the electronic delivery of information by means of information communication technology (ICT), which encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer and interchange of data and information. 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...

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.

Regardless of the term used, the objective is to ensure:

- **Confidentiality**—Data or information are not made available or disclosed to unauthorized persons or processes.

---

**Steve Akridge**, CISM, CGEIT, CISSP
Is owner and president of BorderHawk LLC, a company specializing in cybersecurity and IT risk management integration. Following a 20-year career with the US Naval Security Group Command, Akridge served as the US State of Georgia’s first chief information security officer and later as a technical director with the US Defense Security Service. After leaving public service, he became a private security consultant to a variety of public- and private-sector enterprises, including Wells Fargo, Coca-Cola, and US state and local government entities in the US States of Alaska, Florida, Montana, Nevada, New York and Texas. He has represented the interests of employers and delivered presentations on a variety of information security-related subjects to groups such as the Partnership for Critical Infrastructure Security (PCIS), the US National Association of State Chief Information Officers (NASCIO), the North American Electric Reliability Council (NERC), the US Federal Public Key Infrastructure Steering Committee and the Southeast Cybercrime Institute. Akridge has taught cybersecurity as an adjunct professor at the graduate level and business at the undergraduate level. Additionally, he has co-authored a variety of articles on information protection issues and has been interviewed or quoted on such issues in several publications.
Integrity—Data or information have not been altered or destroyed in an unauthorized manner.

Availability—Data or information are accessible and usable on demand by an authorized person.

Throughout this discussion, the term “cybersecurity” will be used to include all facets of information protection.

What Is a Cybersecurity Program?

Today's enterprise landscape is defined by the people, processes and technology used to manage information. That information is the essential element of most organizations. Therefore, the only reasonable approach to sustainable cybersecurity is to involve an organization's people, processes and technology in the solution. This means that cybersecurity should be perceived as an enterprisewide 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.

A plan of action is aimed at accomplishing a clear business objective. It includes details about what work is to be done by whom and when, and what means or resources will be used. In contrast, programs deliver outcomes, but projects deliver outputs. A program approach to cybersecurity does the following:

- Provides the structure and processes essential to control cybersecurity operations and react to changes related to information risk
- Supports the organization's vision, goals and objectives. The allocation of resources influences the cost and success of the program

from an enterprise perspective, not as part of the IT budget.

- Integrates component parts necessary to power the intended whole, allowing for continual performance optimization both functionally and technically
- Assures adherence to standards and alignment with the business vision, facilitates accountability and management of component projects, and tracks basic component costs together with the wider costs of administering the program

Cybersecurity is not a project, based on the differences between a project and a program:

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

“EFFECTIVE PEOPLE, PROCESSES AND TECHNOLOGY ARE ESSENTIAL TO PROTECT INFORMATION, BUT ANTICIPATING CHANGES IN THE NEED FOR AND USE OF INFORMATION SHOULD BE AN EQUAL CONSIDERATION.”

In most organizations, information need, use and protection are bounded by three functional areas—business management, legal considerations (regulations and contractual arrangements) and IT (figure 2). Business goals change, new legal requirements involving the use and protection of information emerge, and new technology is frequently adopted to support those changes.
Effective people, processes and technology are essential to protect information, but anticipating changes in the need for and use of information should be an equal consideration.

With these things in mind, a cybersecurity program should be viewed as an overarching, enterprisewide sequence of three constantly expanding and contracting activities:

1. **Prevention**—These activities may include security architecture design, security awareness and training, and policy development. In general, prevention encompasses any activity that limits or contains a potentially damaging cybersecurity event.

2. **Detection**—These activities enable the discovery of cybersecurity events. Examples include system log analysis, visitor log analysis and event reporting by users.

3. **Response**—These activities are steps taken to contain the threat and recover business operations. Responses can range from analysis of anomalous but nonthreatening events to efforts to address a data breach or crisis.

It is essential that the cybersecurity program is orchestrated and synchronized with the organization’s business goals, and it must be inherently flexible enough to recognize real-world risk and compliance issues (figure 3). Achieving this synchronization is largely a matter of adopting or defining an inclusive information management control framework and building a working program apparatus based on that framework. In doing so, an organization can recognize information risk and manage that risk in a systematic way.

---

**Information Protection Frameworks, Standards and Regulations**

There are multiple frameworks for managing information risk. Every organization is different and has its own needs and, in some cases, the applicable framework may be predetermined by regulation. Alternatively, a compilation of frameworks and best practices can be cobbled together to create a unique framework. Many information security (InfoSec) authorities have released standards over the years that may help enterprises manage their information security risk. Common standards and frameworks, also known as “best practices,” are listed in figure 4.
Some of the standards listed in figure 4 are recommendations for security practices; others are complete lists of controls that, in the opinion of the issuer, should be met. For example, in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 17799:2005, the ISO/IEC defines guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization. More specifically, it provides recommendations on the following:

- Security policy
- Organization of information security

Cybersecurity Program Functions

According to ISACA:

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.  

For a structured program, cybersecurity governance is the centerpiece from which each of the three activities previously described—prevention, detection and response—must be coordinated. But because critical information is so pervasive in most organizations, other important functions require cybersecurity considerations, too. In addition to core cybersecurity operations, these functions are
planning, project support and risk management (figure 5).

These functions describe the activities necessary to provide basic cybersecurity coverage. In larger organizations, each function may be represented by a separate team; in smaller enterprises, one individual may be in control of everything. The bottom line is that even identical organizations may design and implement completely different cybersecurity programs, but the basic functions will always be the same.

**Governance**

Although organizations often try to relegate privacy and information protection functions to IT management, all parts of the organization must accept responsibility for information protection. This is true because within each organization there are functions that own information, functions that are custodians of information and functions that use information. For example, an employee database may be managed by IT, but the IT team is merely the custodian of the information within that database. Similarly, line managers may access 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 (BoD), managers and internal auditors all have significant roles to play in the adoption and implementation of information protection controls. The BoD must provide oversight of information ownership, protection and policies, and it must shape the corporate culture to enable information protection.

Executive managers must provide leadership to ensure that information protection efforts are supported and understood across the organization. This includes dedicating sufficient resources so that information management controls are effective. Executive managers must continually review activities for improvement, and they are ultimately 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 (e.g., sensitive or critical). Likewise, they must review and monitor the operation of information protection controls to ensure their appropriateness in the face of changing risk and business requirements.

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

A cybersecurity leadership role must be created, and the individual who accepts that role should be empowered to coordinate, manage, recommend and escalate all issues related to business information risk. This executive must have access to all the resources necessary to interpret applicable laws and regulations governing how the organization controls sensitive information. In addition, this executive must advise the board and senior management as to the appropriate organizational perspective on various information risk issues.

**Operations**

The core cybersecurity function for most organizations depends on the following essential activities.

*Prevention of Threatening Events* Activities related to creating, implementing and overseeing safeguards to prevent threatening events typically include the following:

- Establish an information security architecture consistent with the enterprise’s cybersecurity...
governance directions to protect the confidentiality, integrity and availability of information.

- Ensure user and staff security awareness and provide security-related training, including role-based and privileged user training.
- Define and implement information protection processes and procedures necessary to maintain and manage information resources.
- Implement identity management and access control, including physical, digital and remote access.

Detection of Threatening Events
Activities that enable the timely discovery of cybersecurity events typically include the following:

- Define and implement continuous security monitoring capabilities to detect cybersecurity events.
- Develop and implement detection processes to warn of anomalous events.
- Implement vulnerability management. Regularly conduct vulnerability scans to assess system vulnerabilities, and coordinate with IT management on remediation. Conduct red team tests, and coordinate with infrastructure management accordingly.
- Analyze cyberevents by conducting cyberinvestigations to determine cause and effect.

Response to Threatening Events
When a potentially damaging or threatening cybersecurity event is detected, the appropriate cybersecurity incident response plan should be executed. Relevant definitions include:

- Event—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 the execution of malware that destroys data.
- Incident—The culmination of an event or events leading to a judgment that the confidentiality, integrity, or availability of sensitive or critical information or associated information systems may be subject to compromise (the potential for a breach). An incident may include both intrusions (from outside the enterprise) and misuse (from within the enterprise).
- Breach—Definitive loss of control, compromise, unauthorized disclosure or unauthorized acquisition of, and/or unauthorized access to, sensitive or critical information.
- Cybercrisis—An abnormal situation that threatens an organization’s objectives, reputation or viability. These events involve the organization’s ability to ensure the confidentiality, integrity or availability of certain information or information resources critical to its operation. A cybercrisis may be defined as a breach, compromise or disruption of the organization’s critical data or systems.

Components of a cybersecurity incident response plan typically include the following actions:

- Follow response planning protocols in accordance with the defined threat level.
- During and after an event, manage communications with stakeholders, law enforcement and third parties (i.e., vendors, clients, partners) as appropriate.
- Analyze events to ensure an effective response; support recovery activities, including forensic examinations; and facilitate a determination of the impact on the organization.
- Implement immediate mitigation procedures to prevent expansion of an event and to resolve the incident.
- Assure timely recovery from an event and restoration of normal operations (also known as impact reduction).
- Identify improvements based on lessons learned and reviews of existing policies, procedures, guidelines and activities.

Planning
Planning activities to support all aspects of the cybersecurity function typically require the following:

- Research new technology and process changes for potential vulnerabilities.
- Create and maintain a knowledge management function that collects and maintains information.
relevant to the information security program. This may include details about the cybersecurity program and background on threats, vulnerabilities, and tools and templates used to implement the program.

- Assist in drafting and implementing cybersecurity policy and procedures.

Project Support
Project support activities typically include the following:

- Obtain cyber risk guidance on all projects undertaken by the organization.

"THE RISK MANAGEMENT FUNCTION IS THE ENGINE THAT DRIVES THE CYBERSECURITY PROGRAM."

- Clarify implementation questions consistent with the information security policy and the organizational risk tolerance.

Risk Management
Risk management is the ongoing process of balancing business opportunities with the impact of threats that exploit vulnerabilities. The risk management function is the engine that drives the cybersecurity program. It uses industry best practices and standards and best-of-breed tools to determine the value at risk and, thus, the appropriate level of resources earmarked for risk mitigation. Risk assessments are continuously updated, monitored and tracked, with input from the other components. Activities typically include the following:

- Conduct routine internal information risk assessments.
- Conduct third-party vendor information risk assessments.
- Identify specific regulatory requirements (e.g., PCI DSS, the US Healthcare Information Portability and Accountability Act [HIPAA], SOC 2, ISO 27001, DFARS), and ensure conformity.
- Identify a supply chain risk management strategy including priorities, constraints, risk tolerances and assumptions used to support risk decisions.

Managing the Cybersecurity Program Life Cycle

An information security program is never static. There will always be areas to improve, new vulnerabilities to correct, policies to update, assessments to conduct, new technology to incorporate and so forth. The security project management component leverages best practices in the areas of operational performance and project management to organize and manage the projects required for the information security program function. This function creates the organization’s project road maps; originates plans of action; develops and builds consensus 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 is driven by meeting information security requirements, educating people about their responsibilities and building governance structures to ensure compliance, all while monitoring and reporting progress so that policies or requirements can be adjusted appropriately (figure 6).

Figure 6—Cybersecurity Program Life Cycle
This approach should be perpetual. That is, based on conclusions derived from security incident analyses or security compliance assessments, policies and procedures should be refined and education and awareness should be adjusted to better focus on current issues. Then the cycle begins again.

Managing Cybersecurity

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

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

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

Although cybersecurity management should be integrated into enterprisewide decision-making processes, especially when a security project is involved, cybersecurity management must be a time-based decision-making entity. Within cybersecurity, time is the one critical constant in all efforts. For example, the strength of encryption is ultimately based on the amount of time needed to break the code, just as the strength of a safe is measured by the “torch and tool” time needed to penetrate its armor. Similarly, “dwell time” describes how long malware has resided in a system prior to discovery and eradication, thereby estimating the compromise period. Cybersecurity is rarely static.

Conclusion

A cybersecurity program should be much more than a localized collection of prevention, detection and response activities. To be effective, a cybersecurity program must be dynamic. To be dynamic, the program must be elastic in the sense that information governance is an enterprisewide undertaking. Each functional element of the organization is a stakeholder and, therefore, must share responsibility for information use and protection. Information risk, and thus cyberrisk, is a critical subset of the organization’s overall business risk and therefore cannot be isolated as a technology management issue alone.

Endnotes

1 National Initiative for Cybersecurity Careers and Studies, Glossary, “cybersecurity,” USA, https://niccs.us-cert.gov/glossary#C
4 ISACA, Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, USA, 2003