7 Core Elements for your Cybersecurity Strategy

ISOutsource

TABLE OF CONTENTS

INTRODUCTION

The hyper-acceleration of cybercrime and its impact on businesses, their customers, and other users in general is becoming increasingly difficult to manage. Breaches in the workplace are quickly impacting users in their personal and social settings. Traditionally deployed information security solutions are no longer good enough, organizations must approach cybersecurity in a strategic manner. This includes clearly understanding risks and associated issues, understanding the business impact and associated costs, and understanding how to create an effective cybersecurity program that is scalable and extensible for business, risks, and evolving threats.

This paper examines the seven core principles to create strategies for most types of organizations. Strategic foundations are consistent; however, variable implementation and operations require you to identity what works best within your organization.

BEING STRATEGIC

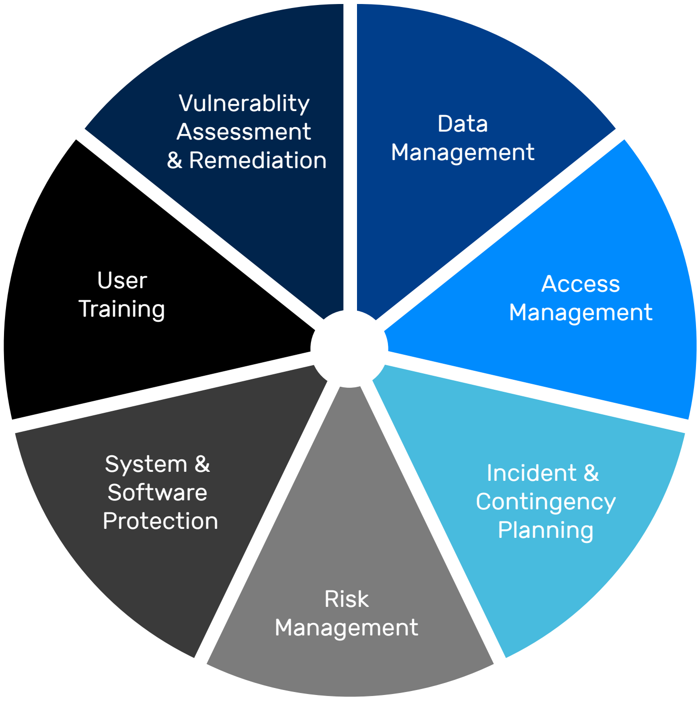
Think strategically; assess all current in-place cybersecurity solutions, understand your business and regulatory requirements, then design a future-state strategic plan. Creating effective cybersecurity strategy plans is straightforward, it's blending the common vision, business, and technical requirements, and aligning with regulatory requirements. The difficulty is determining the correct elements, aligning with standards, and implementation.

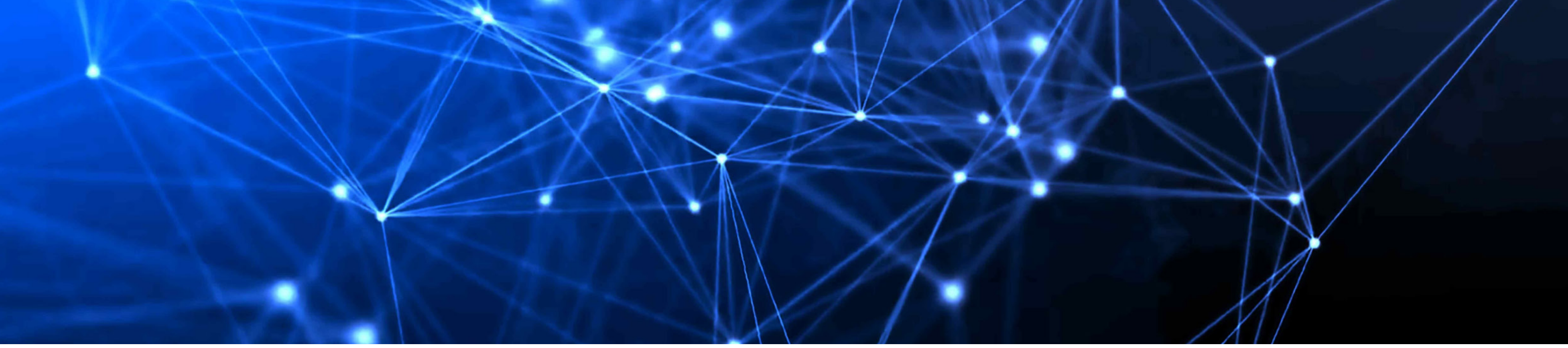
Our approach to creating strategic plans includes 7 cybersecurity strategic elements serving as the foundation for technical, functional, and administrative activities. These elements ensure protection in a scalable manner, accommodating changes to business requirements and evolving threats. Our approach accommodates requirements from all key stakeholders, maturity levels, operational and budgetary constraints, and continued business changes.

The key to successful cybersecurity strategies is designing implementation activities and technical solutions, ensuring consistency with relative importance to objectives and risk. The adoption of strategic elements should be aligned with your current maturity state, with goals to improve.

The 7 cybersecurity elements are appliable to all organizations; the implementation requirements and controls are similar in many organizations; and the implementation activities will vary based on business, technical, and regulatory requirements.

Strategic implementation includes documented policies, programs, procedures, and controls. Documentation creates the formalized path for strategies to become implemented practices.


Vulnerablity Assessment & Remediation
Data Management
Access Management
Incident & Contingency Planning
Risk Management
System & Software Protection
User Training



1) DATA MANAGEMENT

To effectively protect your data, the Data Management Strategy focuses on knowing and documenting your data, users, devices, and systems, enabling your organization to achieve its mission, vision, and goals. Security is a key part of this strategy; it improves alignment between systems management and your risk management protecting confidentiality, integrity, and availability of information.

The shift from on-site data management and storage to Anything as a Service (XaaS) disrupted traditional internally managed data methods by pushing the management to third-party vendors. This simplified many aspects of cybersecurity while increasing risk and complexity in other processes. For example, managing legacy backup tape systems with endless cycles of tape rotation is replaced by letting the XaaS vendor deal with it; this shift heightens the requirements for an effective Vendor Management Program.

Data Management Strategic Activities

The key to an effective Data Management Strategy is knowing your data (and how it's processed) and controlling access to it.

Data Catalog

Create complete data inventory with all attributes, such as data classifications, location, access requirements, and backup/restoration information.

Access Management

Identify all users and automated processes with access to your data (on and off premises), include roles, access level, and restrictions. Identify why users have access; how users access data; and establish process to periodically review users, roles, access types, and data usage. Consider the least-common privilege model, the principal of limiting access to the minimum required to complete a user's job.

Data Processes

Identify all systems with automated and manual access to your data. Understand and limit access to systems following the least common privilege model.

Data Tracking

Document how data moves through your systems, identify and log all automated or manual process for data transformation. Know how your data is leaving your systems, consider preventing all unnecessary data exfiltration. Implement different data restrictions based on user roles and data classifications.

Data Backup

This activity is also addressed in other strategies. Use your data catalog to establish how often your data will be backed up, how you will restore it, and how you will test the systems. Establish Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and Maximum Tolerable Outage (MTO).

3rd Party Management

Document how XaaS providers accesses your data, how the data is backed up/restored, and SLAs for data availability.

2) ACCESS MANAGEMENT

An effective Access Management Strategy reduces costs and risks by ensuring correct access to authorized systems for authorized users. A strategic access management implementation establishes minimal user access, leverages toolsets to manage users, contains automated internal audits, and limits exposure in the event of a breach.

User Access Strategic Activities

Your strategy should include how to limit systems access and manage users for local and remote access. The strategy must be flexible to allow for XaaS variables.

Roles

Define user activities and required access levels, create common roles or groups when multiple users share similar activities. If applications or systems permit, create a role or group and then assign users to designated roles/groups. Data should be classified; the classification should identify the permissioned access roles.

On/Off Boarding

Create a process for consistent user on/offboarding (provisioning). A consistent onboarding workflow includes required organizational approvals, background checks, new user training, and asset allocations. Automated process ensures completion of all checkpoints and documentation. A swift and efficient onboarding process reduces risk while creating a good experience for new users. Similarly, a documented offboarding process immediately that removes all authorizations must be established to ensure unauthorized access to systems does not occur after users are offboarded.

Multi-Factor Authentication (MFA) or 2 Factor Authentication (2FA):

The login requirement with 2 different elements of identification. This often includes a password and secondary identification method, such as pin code, code sent via SMS, picture ID, or other personal information. This has become the minimum standard for many organizations.

Single Sign On

The user logs into a single system, the system provides credentials to other systems.

Identity Access Management (IAM)

An integrated solution aggregating all user allocations into a single location. The user accesses the system with a single sign on (with MFA) and receives access to associated resources. The IAM tool can control time/date access, location access, on-premises solutions, XaaS, and file-level permissions. An IAM can quickly onboard new users and terminate instantly; IAM provides the most comprehensive access management and security possible.

Elevated or Administrative Privileges

All administrative activities (user management, systems management, administrative tasks) should be completed by users with Elevated or Administrative access. Likewise, only administrative tasks should be completed with this profile. This role must use MFA with password complexity. This role should be guarded; this is a popular exploitation by bad actors.

3) INCIDENT & CONTINGENCY PLANNING

Unplanned activities and incidents occur, no matter how well you built or maintain your systems. Your planning needs to address all three major categories: Business Continuity, Disaster Recovery, and Incident Response. Your strategic approach needs to consider a myriad of risk-based responses, likelihoods, and impact. You must consider additional variables common to XaaS risks when designing and implementing your response programs.

Incident & Contingency Management Strategic Activities

Your response strategy addresses business interruption, disaster recovery, and cybersecurity incidents. The key to all strategic activities focuses on preparation leading the method for prompt recovery.

Business Continuity Planning (BCP)

The BCP plan focuses on interruption to normal business workflow; it addresses multiple types of interruptions, such as technology, financial, facilities, and human resources. The plan focuses on business processes, resource requirements, workarounds, and return to normalcy. Examples include addressing short-term internet outage and an organization’s ability to serve its customers or if users are unable to work in a normal office due to a pandemic. Both examples address interruption to normal workflow and the organization’s response. Written plans should include all critical, essential, and important workflows; technology and physical requirements; minimal resources; and alternative plans. Plans and workflows should be periodically reviewed to ensure technical responses are aligned with expectations. Plans should be exercised periodically to ensure alignment business and regulatory requirements. Consider how XaaS outages and recovery impact your normal operations.

Disaster Recovery Planning (DR)

The DR plan addresses technology systems recovery after interruption. This plan addresses critical business and technology systems, on premises, hosted, and XaaS. A baseline requirement is data backup and ability to recover. These requirements are generally identified in the BCP. Data and system restoration ranges from simply restoring a backup to having to restore in an alternate facility. Plans should include full topography documentation, all technical dependencies, vendor dependencies, and all elements to recover. Consider how XaaS outages and recovery impact your ability to recover.

Incident Response Planning (IR)

The IR plan is the response to cybersecurity attack or data-loss incidents. The plan's goal is to reduce impact and expedite recovery. The plan defines incidents, guides responses, and outlines return to normalcy. The IR specifically identifies roles and responsibility during and after the event, establishes communication criteria, and addresses interaction with law enforcement.

Communications

All three scenarios require communications with key stakeholders and customers. Each plan should include outlines of communications, with sample content already created and approved by legal counsel. Highly regulated organizations need to comply with customer notification in accordance with regulatory requirements, often within a specified time period.

Testing

BCP-DR-IR should be periodically tested with different scenarios and participants. This should include non-impactful activities, such as monthly tabletop exercises, as well as high-impact activities, like full system restoration. Each test activity should document the test event, results, lessons learned, and improvement opportunities.   Effective training and testing will review process and technical vulnerabilities, often leading to system and process hardening.

4) RISK MANAGEMENT

Risks are considered anything impacting the goal, mission, operation, or activity; this includes human, technical, or acts of nature, accidental or intentional, and direct or indirect. Major risk categories include business, financial, technical, human, and reputational. Most of the time a risk will impact multiple or all categories. An effective risk management strategy includes risk considerations for all activities. Healthy risk awareness leads to lower risk profiles while improving organizational decision making. Integrate your organization's priorities, constraints, tolerances, and assumptions into your risk strategies.

Risk Management Strategic Activities

A comprehensive strategy addresses risks wholistically with strategic and operational responses.

Risk Identification:

The foundation of any program is to identify the risk. Consider all risks under your control and controlled by third party, and include all the elements of uncertainty. Create a comprehensive list of risks. The first version of your list might be high level. That is OK, risk identification a continuous activity, risks may be further refined at a later time.

Risk Register: This key component formally documents the risks and related management processes. It should be reviewed periodically to ensure identified risks are appropriately managed. Critical risk and related dispositions should be reported to management. It should contain a Risk Rating for all risks.

Risk Rating:

The following Risk Register elements enable consistent evaluation and management. Two sets of ratings occur, Inherent Risk (without controls in place) and Residual Risk (the risk with controls in place).

Impact - inherent: Determine the impact to the organization if the risk caused an incident. Rating ranges from low impact to high.

Likelihood - inherent: Identify the chances of occurrence. Ratings range from low to high.

Risk Treatment: Risk responses generally are broken down into four categories. Mitigate – reduce the likelihood or the impact; however, not completely remove. Eliminate - remove the activity or the risk completely from the environment. Accept – accept the risk because an alternative does not exist or the costs for a different treatment is excessive. Transfer – move the risk or the costs of a risk to a third party, such as insurance company.

Risk Control: The activities based on the risk treatment. For example, if you may use an anti-virus solution because the computer must be connected to the internet. The solution mitigates the likelihood and impact if a virus occurs. Conversely, if you do not allow the computer on any network, you eliminate the likelihood and impact from occurring. You may also choose to transfer the impact to a third party via an insurance policy.

Control Effectiveness: An assessment of current control effectiveness. Periodic review of risk registry entries should occur to evaluate control effectiveness. Ratings range from Poor to Acceptable.

Residual Risk: A calculation of Inherent Risk multiplied by Risk Control Effectiveness, establishing a score. This score is used to identify risks requiring additional remediation.

Risk Management:

The Risk Register is a valuable tool for establishing and tracking risks when implemented organization wide. It is a valuable tool for planning; it helps determine priorities. It should be included in project management, daily operations, and continuous improvement activities.

5) SYSTEMS AND SOFTWARE PROTECTION

Systems and Software protection is often referred to as IT Operational Strategy; it establishes the framework for managing all technologies, including on and off premise, physical and virtual hardware, enterprise, and user-issued equipment. The core principle is maintaining all systems in alignment with business requirements and risk. Alignment is essential among business and IT principles, communications, and operations.

System and Software Protection Strategic Activities

Create a strategy aligning business requirements with cybersecurity operations. Establish operational process protecting all data, systems, and software enabling and enhancing business operations.

Business Relationship:

Establish a relationship between business units and IT; focus on strategic initiatives, understanding priorities, and business partnership. Establish an IT Steering Committee focusing on organizational requirements. Align IT with the mission, objectives, stakeholders, and activities. Leverage cybersecurity roles, responsibilities, and risk management decisions to enable business operations; ensure cybersecurity enhances, not limits business operations. Operate IT in a single vision with the organizations through relationships and transparent activities.

Security Policies:

Create formal IT cybersecurity policies addressing purpose, scope, roles, responsibilities, management commitment, and coordination among organization entities. Maintain processes, procedures, and standards to protect information systems and assets.

Maintenance:

All maintenance, updates, and repairs of information system components are performed consistent with policies and procedures. Maintain all systems aligned with industry best practices and manufacturers' recommendations.

Protective Technology:

Actively manage all cybersecurity solutions ensuring security and resilience of systems and assets, consistent with related internal and external policies, procedures, and agreements.

Security Continuous Monitoring:

Monitor information system and assets identifying cybersecurity events and verify the effectiveness of protective measures. Leverage system log files and tools to ensure security effectiveness.

Standards or Regulations:

Considering using a recognized standard to create the cybersecurity program and related policies, practices, procedures, and controls. Ensure adherence to all regulatory requirements; review and validate on a periodic basis. Be aware of new regulations impacting your operations.

Be Proactive:

It’s too late to be proactive after an incident. Build and maintain your environment with appropriate tools ensuring you know what is occurring. Establish a periodic testing plan to validate your preparedness. Monitor your XaaS to ensure the appropriate cybersecurity measures are in place and tested. Plan all changes to security items related to systems, networks, devices, and software owned, leased, or subscribed to by the company.

Budgeting:

Leverage your strategy and information systems to create effective budgets to protect and operate your systems and solutions.

Business Relationships: Maintain strong relationships with business units and operate an IT Steering Committee to leverage business requirements to budget requirements. Understand operational and project costs tying budget to operational requirements. Consider show-back or charge-back accountability tying IT costs to business operations.

Risk Management: Use the outcome of your Risk Analysis to budget requests and priorities.

Audit and Assessments: Tie findings to business requirements, IT operations, and cybersecurity costs to specific outcomes.

6) USER TRAINING

Managing user cybersecurity vulnerabilities requires specific strategies. A strategic user training plan extends past traditional cybersecurity briefings into protecting users at home and social settings. Effective training strategies include ongoing training aligning with business and technology requirements, emerging threats, and local vulnerabilities. Specialized, ongoing training should be included for Power Users, System Admins, Program Owners, and high-risk systems.

User Training Strategic Activities

The goal of the strategic training plan is to shape user behavior protecting business systems and users' personal and social activities. All users need to be aware of risks and demonstrate good cybersecurity hygiene.

New User Training:

All users should receive training prior to receiving system access credentials. This ensures alignment with organizational requirements. Non-employees (vendors, 1099's, etc.) should receive this training, ensuring understanding and alignment with organizational expectations. The Acceptable Use/User Responsibility guidelines supplemented with safe-computing guidelines are ideal for training curriculum.

Annual Refresher:

All users should receive annual refresher courses based on changes to the Acceptable Use/User Responsibility guidelines. Annual training should also focus on current events or incidents that the organization experienced.

Ongoing Training:

Ideally, organizations devote time each month to communicate a heighted cybersecurity awareness activity. This can be in the form of a quick 2-minute cybersecurity update in meetings, emails, newsletters, or blogs. Constant, organization-specific cybersecurity updates demonstrate the importance of cybersecurity in an easy-to-consume manner. Avoid lengthy, overly technical, and dry security training.

Training Tools:

Leverage ready-made cybersecurity training programs (Training as a Service). Many programs include curriculum designed for different knowledge levels, allow you to insert your content, and track users completing the training.

User Testing:

Many Training-as-a-Service programs offer user testing. An example of user testing is Phishing Tests. The system sends random users Phishing tests. This test re-enforces rules such as “don’t click on non-validated links in email.”

Protect the Organization, Protect Your Personal Life, Protect Your Social Life:

An increasing number of cyberattacks are attacking one aspect of a user’s life, then using the found vulnerability to attack another aspect of a user’s life. All training should include how to protect a user when not in the organization.

Train Users Beyond Cybersecurity:

Training should include regularly and occasionally used systems. Failure to properly use systems often result in error and vulnerabilities. Often, users create workarounds to input or transfer data because they do not understand built-in system automation.

7) VULNERABILITY ASSESSMENT & REMEDIATION

Cybersecurity never rests; your strategy must address the constantly changing threat, risk, and vulnerability landscape. Include comprehensive toolsets and processes for assessing and remediating vulnerabilities.

Vulnerability Management Strategic Activities

Create an extensible and expandable strategy addressing threats to business activities, technical solutions, and regulatory requirements.

Scanning:

Implement a periodic, automated solution(s) for scanning and reporting vulnerabilities. The solution should include automated updating of its vulnerability listings, rank vulnerabilities, and provide detailed reports as well as executive summaries. The solution should be clear and precise, making it easy to make decisions about remediation. Re-scan after all major environmental changes. Include all XaaS as much as possible; include vulnerability management in your vendor management process, ensuring data protection outside of your environment.

Remediation:

Vulnerabilities must be addressed immediately, ranked, and scheduled for remediation in accordance with risk, business impact, and regulatory requirements. Remediation decisions and activities must follow your change management processes, even emergency patching. Consider re-scanning after major remediation activities.

Log Management:

Leverage log activity in your environment to help identify vulnerabilities and anomalies. Use an effective Security Information and Event Management (SIEM) solution to understand what is occurring in your environment. Include periodic tuning, leveraging the SIEM’s features to understand your environment’s activities and vulnerabilities.

Risk Strategies:

A strategic approach to managing risks includes a full understanding of internal and external risks, with the likelihood and impact for each risk. Consider maintaining a complete Risk Matrix, as described in the Risk Management Strategy section.

Prevent:

Periodically evaluate your vulnerability program to determine its effectiveness at detecting vulnerabilities. Is your program actionable? Did an incident occur due to your vulnerability program deficiencies?

Penetration Testing:

Conduct periodic external pen tests against your environment to identify vulnerabilities and security holes. External pen testing can also detect configuration vulnerabilities and technical errors created by support staff.

iSOutsource

hello@isoutsource.com

(800) 240-2821

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™