tracesecurity
Compliance, simplified.

Whitepaper

Information Security Policy:
What Every Organization Needs

Mitchell Bearry
Information Security Analyst

Introduction

Most financial organizations are already familiar with the concept of an Information Security Policy – a document used to outline the standards and procedures to be performed by a company for the protection of information, particularly related to cybersecurity. However, one thing I have noticed over the course of time when conducting risk assessments and IT audits is a disparity in what items an Information Security Policy should include. The purpose of this paper is to introduce the concepts and topics a proper Information Security Policy needs, backed up by guidelines set by NIST and FFIEC, and looked for during audits performed by Information Security Analysts such as myself.

Elements

While the elements that make up a solid Information Security Policy will vary depending on each organization's size, business structure, and needs, there are common factors that each business should consider for inclusion. The following is a list of topics I look for within an organization's Information Security Policy when performing IT audits:

- Purpose and Scope
- Roles and Responsibilities
- Risk Assessment/Management Policy
- Vulnerability Assessment/Management Policy
- Change Management Policy
- Patch Management Policy
- Data Classification Policy
- Backup Procedures
- Remote Access Policy
- Physical Security and Access Control
- Logical Security and Access Control
- Privacy Expectations
- Employee Agreement

While it is certainly acceptable to maintain these as their own individual policies, by incorporating these procedures into the Information Security Policy, an organization can help ensure that they are approved simultaneously alongside the rest of the Information Security Program. It also reduces the number of separate documents that need to be reviewed, updated, and approved, which aids in preventing any of them from falling through the cracks and escaping notice by IT personnel and executive management.

Description of Elements

Purpose & Scope

This section is designed to be the first in the document, ideally located on page one. It should outline the reason for the policy and the Information Security Program as a whole, as well as the scope that the policy will cover. Statements within this section usually define the organization's responsibility to protect member information and prevent unauthorized access to this information.

Any ancillary information, such as a table marking the revision history for the Information Security Policy, as well as the latest approval dates by the Board of Directors can also be included here.

Roles & Responsibilities

This next section lists the employees responsible for the Information Security Program and defines their roles. This should consist of System Administrator, IT Manager, or other personnel responsible for developing and maintaining the Information Security Program and all its associated functions. Their duties will typically also include the creation and modification of the Information Security Policy.

In addition to the IT roles being documented, it is also important to identify the involvement of the CEO, Board of Directors, and/or other executive positions of the institution. The CEO should be responsible for assigning the previously mentioned duties to IT personnel and ensuring that this process is performed correctly. The Board of Directors should review the Information Security Policy and any updates to it on at least an annual basis and approve the document for use.

Risk Assessment / Management Policy

This section of the Information Security Policy is designed to outline the organization's process for identifying, assessing, managing, and documenting risks, threats, and vulnerabilities to the institution's systems and services. The section should define which personnel are responsible for each step of this process, whether that be analyzing and documenting risks through internal risk assessments, working with vendors for independently performed risk assessments, documenting the results and mitigation actions to track remediation, or approval of the results and procedures by the Board of Directors or other governing stakeholders. It should also include any details of these processes necessary for them to be performed, such as the software used to track remediation in the event that an employee unfamiliar with the process needs a standard to reference. The institution's risk tolerance should also be defined to ensure that all employees are aware of the level of acceptable risk.

However, it is important to note that specific instructions or other information sensitive to the organization's identified risks should not be detailed here. Any instructions on the use of software or the exact methods, especially examples of existing risks and threats to the organization, should be kept instead in a separate document that records the steps for resolving vulnerabilities. This policy only serves as a high-level outline of the methodology for assessing and managing risk.

Vulnerability Assessment / Management Policy

A vulnerability assessment and management policy is very similar to the risk assessment and management policy. In fact, these procedures are often combined to form a single section within the Information Security Policy governing the mitigation of risks and vulnerabilities. Just like the risk policy, this section should outline the high-level process for identifying vulnerabilities through periodic assessments by a third party, or through regular vulnerability scans run internally. It should also then detail the procedures for mitigation of the vulnerabilities, and the level of tolerance for accepted vulnerabilities.

Change Management Policy

Establishing a change management policy helps to reduce the number of errors or bugs caused by changes to the organization, including its systems, business operations, policies and procedures, and all other modifications. There are several factors that contribute to a thorough Change Management Policy. The below list contains the most important items to include, as well as their purpose.

- Personnel: The policy should define the role of all employees regarding change management. This includes which staff members are authorized to make changes, the employees authorized to approve changes, and the responsibility of executive management and the Board of Directors (or similar stakeholders) in reviewing and approving the policy.’
- Baseline configuration: A standard should be established for each category of technical assets regarding the initial settings and configurations applied prior to its installation. These requirements, and the instructions for implementing them, can be placed within its own procedure document if desired rather than outlining the entire process within this section. If this is done, make sure to include sufficient references to where these additional documents may be found.
- Change control solution: There should be a solution in place to log and track changes made. This can be accomplished through the use of ticketing software, a spreadsheet, or another software solution. Whatever the chosen mechanism is, it should have the capability to record the following information for each change made:
    - The details of the change made, including comments by personnel performing the change
    - The person who requested the change
    - The person who approved the change
    - The date (and time if possible) of the change
    - The status of the change (in progress, pending, complete, etc.)
- Testing: Procedures should be defined for conducting any testing necessary prior to implementing the change to ensure that the organization is not adversely affected by applying the change. Testing should also be performed after making the change to verify that all affected systems and services are still functioning normally.
- Additional Documentation: If a ticketing software is not used to request and approve changes, change request forms should be maintained to allow for the review and approval of proposed modifications prior to their implementation. The policy should detail where these forms, as well as any other needed documents for change management are located and the process for utilizing them.

Patch Management Policy

While it may first appear that the patch management policy falls under the same umbrella as change management and should be included within its procedures, it is typically defined as a separate section due to it serving an additional purpose – to ensure mitigation of vulnerabilities. In this way it functions as a combination of the change management and vulnerability management procedure sections. In the same way that a software solution may be used to track changes, an automated patch management solution is often used to log applied patches, test the updates prior to deployment, and alert appropriate personnel when a new patch or update for installed software and applications is available.

Since most remediation of vulnerabilities on systems consists of updating the affected service or software to the latest version, establishing and maintaining a software solution to automatically apply both operating system and third-party application patches across all devices is an important addition to any organization's network, and the standard for using this software is an important addition to the Information Security Policy.

Data Classification Policy

This is a big section, and one that may not be feasible for many smaller organizations to implement due to the amount of time it takes to create and maintain. However, it serves as an important component of an Information Security Policy in that it enables administrators to better separate employees by job role to avoid unauthorized access to data outside their responsibility should an employee's data be compromised.

A table is typically included to define the categories in which information can be classified, such as public, private, and confidential. Once data can be assigned their corresponding types, instructions can be listed regarding which personnel are allowed to communicate each type, whom they are allowed to provide the information to, and the secure methods for doing so.

Backup Procedures

Backups are one of the most important aspects an organization can implement to substantiate their business continuity program. With the increasing prevalence of ransomware attacks, having backups in place for all sensitive and critical data is essential to ensuring a complete recovery following an incident.

With how crucial this capability is to the business, procedures must be defined to set the standards for the backups, including how they are performed, how frequently they occur, the encryption levels required, the restoration process, and all other requirements. This will help make certain that following an event, the institution is able to successfully restore their business operations back to normal.

Remote Access Policy

Given the recent pandemic resulting in larger than normal and ever-increasing numbers of employees working from home, it is more critical than ever that procedures and standards for remote access be established, which can most easily be added to the Information Security Policy.

A Remote Access Policy is responsible for dictating the standards for how remote access to the corporate network is requested, approved, provided, maintained, logged, revoked, and otherwise managed in its entirety. The software used, such as VPN settings and configuration requirements, monitoring solutions in place to record access and activity, contact information for vendors to perform setup, and all other necessary dependencies to enable, maintain, and disable remote access for employees should also be defined.

Physical Security & Access Control

The standards that govern this aspect of security is likely already in place in some form or fashion, and most organizations, especially financial institutions, are probably already familiar with at least a few of the procedures governed by this section of policy.

Physical security is not a new idea; people have been locking doors, building walls, and controlling access to money and other valuable treasures for thousands of years. However, what this section in an Information Security Policy focuses on the physical side of security when it comes to protecting data, not the money in the vault. In today's world, information is as much a currency as cash. Therefore, it is critical to implement the physical controls, and the standards to govern those controls, to ensure that this factor is protected from cyber criminals utilizing social engineering and other techniques to gain access.

Some of the controls typically put in place to serve this purpose are locking mechanisms, whether they be physical keys, or forms of electronic access control such as combination locks, RFID badges and readers, and key fobs. Mantraps, security guards, and turnstiles are also examples of physical controls used to manage access.

While preventing access is important, if these controls are circumvented, controls should also be in place to monitor the physical environment to identify any potential attackers, and to obtain evidence of perpetrators after the breach has occurred. Security cameras, motion sensors, security alarms, and other systems help log entry to facilities and serve as forensic evidence in any future investigations.

Logical Security & Access Control

In tandem with protecting the physical data, electronic data must also be guarded against the threats posed by cyber criminals on a daily basis.

The amount of possible logical access controls is too large to go into great detail; however, Access Control Lists (ACLs) for firewalls, Intrusion Prevention Systems (IDSs), Security Information and Event Management (SIEM) solutions, Network Access Control (NAC), antivirus programs, and endpoint protection solutions are just some of the controls that can be implemented to filter authorized individuals from the unauthorized, and detect, if not prevent altogether, access by potential attackers.

The Information Security Policy should outline which systems are in place, the personnel responsible for managing them, and any expectations regarding the details of how access is controlled. For specific instructions on operating these software solutions, references to manuals or other procedure documents should be made, rather than including the highly technical details within the policy itself.

Privacy Expectations

While this section is most often included within the separate Acceptable Use Policy, I have seen cases where it was contained within the Information Security Policy. The requirements defined here should explain what personnel can expect regarding their privacy when it comes to email, internal messaging, video conferencing, the Internet, and all other forms of communication. Most often, this is a mere statement to indicate that employees have no right to privacy while utilizing the organization's computer systems.

Employee Agreement

Finally, to aid in ensuring compliance with all the standards and procedures defined within the Information Security Policy, contained within the document should be a means for employees to provide written evidence that they agree to the terms set forth by the policy, as well as the consequences for violating the policy. This agreement signed by both the organization's representatives and the newly hired employee can then be placed in the personnel file for the employee and kept by HR. Additionally, on an annual basis, or sooner if changes are made, all employees should be required to resign the Information Security Policy to reaffirm their compliance.

Conclusion

While certainly not a comprehensive list of all topics an Information Security Policy should cover, the categories put forth by this paper provide a good baseline for an organization to create their first version of the policy. Additionally, any organizations that already have an Information Security Policy may find topics that their plan does not currently cover, and ways in which the existing document may be improved.

Lastly, having the Board of Directors or other stakeholders approve this policy on an annual basis and whenever changes are made will ensure that the standards outlined within are under the purview of a governing body and consistent with the organization's goals and business philosophy.