2017

Needs Assessment Results

Confidential

This document contains the summary results of the Net Reaction Needs Assessment taken by your organization. This snapshot report is intended to quickly assess the current state of your Information Security Program by measuring your practices, policies and procedures against both industry standard best practices and applicable compliance legislation.

# Introduction

Thank you for taking the time to complete this Needs Assessment Survey. We look forward to helping you understand your own unique strengths and needs. Over the next few pages we will examine your answers in relation to how they contribute to your overall threat profile. This report will help you understand what risks your business face, and make suggestions for improving your Information Security Program.

Many organizations report feeling a bit overwhelmed after reading this report. This is normal when you are starting to build your Information Security Program. Rest assured that you are not alone in this feeling, and that it is easy to overcome it once you get started in addressing your particular needs – especially when you have someone to guide you through the process.

It should be noted that this Needs Assessment should not be substituted for a full risk assessment. For this assessment, we are relying solely on information you have provided us, and have not done anything further to verify this data.

Finally, we welcome the opportunity to discuss this report with you. We know that sometimes starting down the path to securing your information seems fraught with obstacles. We have helped thousands of clients secure their information. And, we will be happy to help you get started in securing yours.

# Overview of Results



**Overall Risk Level: Medium - Review as Necessary**

**Overall Risk Score: 61 out of 100**

## Information Security Fundamentals

Information Security can seem very complex. For most organizations however, there are some fundamental items that when implemented correctly will cover most of your Information Security needs. Every organization, regardless of size or complexity needs to have these items in place. Because of this necessity, Net Reaction uses this as a starting place for assessment. As a practical take away, if you find yourself deficient in these fundamentals, you need to start here before focusing elsewhere.

|  |  |  |
| --- | --- | --- |
| **Assessment** | Risk Assessment   * Risk Assessment is the critical tool for understanding the threats to your organization. You can’t protect what you don’t understand. Risk Assessment is the first step that any organization should take in developing an Information Security Program | **Deficient** |
| **Policies & Procedures** | Information Security Policy   * Describes what information needs to be protected and why, expresses management’s commitment to protecting the information and describes to the reader how the information is to be protected | **Deficient** |
| Acceptable Use Policy   * Describes what actions the reader may and may not take in working with and handling the organization’s information | **Deficient** |
| Employee Handbook   * Expresses the organization’s expectations of the reader as conditions of their employment | **Passing** |
| Background Screening Policy   * Gives the organization the employee’s permission to conduct appropriate background checks as a condition of their employment | **Deficient** |
| Confidentiality Policy   * Explicitly states to the reader that all information encountered during their employment is the property of the organization | **Deficient** |
| **Technical Controls** | Firewall Policy   * Firewalls are necessary for anyone storing sensitive information on their corporate networks | **Passing** |
| Wireless Policy   * Wireless networks should be appropriately secured on networks where sensitive information is present | **Passing** |
| Password Policy   * The selection of appropriately strong passwords is one of the most fundamental, yet effective information security controls | **Passing** |
| Data Classification   * Data should be classified according to sensitivity and protected accordingly | **Deficient** |
| Remote Access   * When used, remote access points need to be appropriately configured and secured | **Passing** |
| Secure Disposal of Information   * Information and media must be appropriately destroyed before disposal or reuse | **Deficient** |
| **Other Controls** | Vendor Integrity Assessment   * The vendors and third parties you work with are critical in the protection of your information. Your security doesn’t matter if they don’t have appropriate controls in place. | **Deficient** |
| Incident Response Plan   * Incidents happen to even the most prepared organizations. An incident response plan is critical in minimizing the damage to your organization | **Deficient** |
| Employee Training   * You can’t do what you don’t know. Your organization must communicate its expectations to your employees through training. | **Deficient** |

# Detailed Risk Analysis

The following sections will analyze your strengths and needs in each of the focus areas of Information Security. Each focus area is important and contributes to the overall effectiveness of your Information Security program. Focusing too much on one area while neglecting another area can leave your organization vulnerable to information crimes.

It should be noted that this Needs Assessment is meant to give the user a quick snapshot of their Information Security Program, and is not intended to replace a full enterprise risk assessment by a certified auditor.

## Focus Area 01 – Risk Assessment

Risk assessment is the foundation of information security planning. If your organization’s Information Security Program is going to be effective, the program must address the unique risks faced by your organization. Risks must be fully identified and understood before effective mitigation strategies can be developed. Risk assessment addresses both the process of identifying vulnerabilities and threats as well as the probabilities of their occurrence and potential impact.

Your Information Security Program should include at least the following:

* A framework for the identification and quantification of risks to your organization
* A strategy for developing mitigation strategies to address risks to your organization
* Periodic review and update of your risk assessment

|  |  |
| --- | --- |
| **Risk Level:** | Medium - Review as Necessary |
| **Your Score:** | 65% |
| **Recommendations:** | * Consider formalizing your risk assessment framework |

## Focus Area 02 – Information Security Policy

Documentation of policy is imperative in outlining the principles of any Information Security Program. These policies address management directives for establishing information security for the organization, identify relevant contracts, laws and regulations constraining the organization, and sets procedures to be used in day-to-day operations.

An effective set of Information Security policies should include at least the following:

* Establishment of an Information Security Policy
* Establishment of an Employee Handbook
* Establishment of a Review Schedule for appropriate policies

|  |  |
| --- | --- |
| **Risk Level:** | High - Immediate Attention Needed |
| **Your Score:** | 33% |
| **Recommendations:** | * Adopt a formal Information Security Policy * Adopt a formal Acceptable Use Policy |

## Focus Area 03 – Program Management & Support

All information security responsibilities should be defined for employees and addressed appropriately with external parties. An effective Information Security Program requires a supporting structure within the organization as well as necessary controls for customers, contractors, or partners to sustain a successful information security program.

Your Information Security Program should include at least the following:

* To organize the support structures for an effective information security program
* Ensuring management’s support for information security
* Coordination of information security roles and the allocation of responsibilities among staff
* Establishment of authorization processes
* Establishment of Non-Disclosure policies and confidentiality agreements
* Establishment of relationships with external parties and special interest groups
* Management of external relationships

|  |  |
| --- | --- |
| **Risk Level:** | High - Immediate Attention Needed |
| **Your Score:** | 47% |
| **Recommendations:** | * Formalize your individual pieces of a program into a formal Information Security Program * Consider implementing a formal update schedule for your organizational policies * Consider having an outside third party review your organization's Information Security posture on a periodic basis * The methods that vendors and third parties use to protect your data are as important as the method and controls you use. Assess your vendors' Information Security programs before conducting business * Consider making the protection of your organization's information a part of your vendor contracts |

## Focus Area 04 - Asset Management

Just like risk assessment, you can’t protect something if you don’t know you have it. As an essential part of risk management and disaster recovery, an inventory of assets and information should be maintained by the organization. Without it, the organization has no idea what it is protecting. An effective program should contain guidelines for data owners, classification guidelines, labeling and handling guidelines and establish the acceptable use of information.

Your Information Security Program should include at least the following:

* Establish an asset inventory
* Implementation of classification guidelines
* Identifying owners for the organization’s information and assets
* Establishing Information Labeling and Handling Policies
* Establishing an Acceptable Use Policy

|  |  |
| --- | --- |
| **Risk Level:** | High - Immediate Attention Needed |
| **Your Score:** | 5% |
| **Recommendations:** | * Consider formalizing your Data Classification Guidelines * Organizational assets and information should be clearly labeled and identified according to your Data Classification Guidelines |

## Focus Area 05 - Trustworthy Human Resources

Protection of information cannot be expected by default. Employees, contractors, vendors and other related third parties each have obligations to protect your organization’s information. Beginning with trustworthy personnel, the organization should offer training for defined information security expectations and have a disciplinary plan for handling information security incidents.

Your Information Security Program should include at least the following human resource concerns:

* Documentation of roles and responsibilities
* Establishment of a background screening policy
* Review of Terms and Conditions of employment
* Implementation of Information Security Awareness, Education and Training
* Establishment of formal disciplinary and termination processes

|  |  |
| --- | --- |
| **Risk Level:** | High - Immediate Attention Needed |
| **Your Score:** | 23% |
| **Recommendations:** | * Consider revisiting Information Security topics with employees through periodic Education and Awareness sessions or training * Consider revoking terminated employees access privileges before they leave the premises for the last time - This is especially critical in terminations where the former employee had access to sensitive data * Consider making background screening a formal part of your hiring process - The benefits far outweigh the costs * While having a confidentiality statement in your Employee Handbook is completely acceptable, many organizations prefer to have employees sign a separate formal Confidentiality Policy to highlight the importance of protecting sensitive information |

## Focus Area 06 - Physical & Environmental Security

Proper concern should be given to physical and environmental threats that are either natural or man-made. Everything from the physical perimeter, placement of equipment storing sensitive information and contingency plans for environmental disasters must be assessed. This section highlights characteristics to consider for protecting the organization’s information security from such issues.

Your Information Security Program should include at least the following:

* Assessment of the physical security perimeter
* Evaluation of physical entry controls, office security, external and environmental threats, public areas and loading docks, supporting utilities and cabling
* Assessment of equipment security located offsite
* Establishment of Information Disposal and Reuse policies
* Controlling the removal of property

|  |  |
| --- | --- |
| **Risk Level:** | Low - No Action Required |
| **Your Score:** | 100% |
| **Recommendations:** |  |

## Focus Area 07 – Information Technology Communications & Operations

Today’s business environment relies on networked computer systems to retain, process, and produce immense amounts of information. Attention needs to be given to ensuring that these assets protect your organization’s information as opposed to creating a liability. Appropriately secure systems need to be properly configured, have documented operating procedures and audit trails.

Your Information Security Program should include at least the following:

* Evaluation of operating procedures
* Establishment of operating policies including change control, segregation of duties, separation of production systems, capacity management, system acceptance, malicious code, mobile code, information backup and media disposal
* Review of network controls, electronic messaging, ecommerce, interconnections of business information systems and online transactions
* Establishment of audit logging and the protection of log files

|  |  |
| --- | --- |
| **Risk Level:** | Medium - Review as Necessary |
| **Your Score:** | 74% |
| **Recommendations:** | * Careless disposal of information is a leading cause of data breaches. Make sure that all media and information is securely destroyed before disposal or reuse * Consider setting your antivirus solution to update and run at least once per week on your workstations. * Consider implementing formal change control procedures to evaluate and if necessary roll back changes made to the organization's systems * Consider archiving audit logs for all user activity as appropriate. Audit logs make both troubleshooting and investigations easier and less time consuming. * Assign someone to review your audit logs on a periodic basis. Many instances of fraud have been uncovered by a casual glance at log files. * Test your backup media from time to time, especially if you are using cassette media. Backup media has a finite lifespan and must be replaced periodically. * Consider whether you really need sensitive personal information to be stored on laptop computers. In cases where the answer is yes, continue with whole disk encryption. * Consider whether or not business applications really require sensitive personal information to be collected via the web. In cases where the answer is yes, ensure that you continue the use of appropriate encryption. * Consider formally testing your websites for common vulnerabilities on a periodic basis. * Consider whether or not your business really needs to store credit card information. In cases where the answer is yes, continue the use of appropriate encryption. |

## Focus Area 08 - Access Control

Access to the organization’s information should be restricted based on classifications and the requirements of the Information Security Policy. This section examines this integral issue from general policy to the specifics of password selection and timeout controls.

Your Information Security Program should include at least the following:

* Establishment of access controls
* Management of user registration and access privileges
* Protection of unattended equipment
* Controlling use of network services through authentication, equipment identification, secure logon procedures, session timeouts and limited connection times
* Protection of network equipment through disabling remote management ports
* Segregation of networks
* Sensitive system isolation
* Controls for employees who work remotely

|  |  |
| --- | --- |
| **Risk Level:** | Medium - Review as Necessary |
| **Your Score:** | 90% |
| **Recommendations:** | * Require your employees to secure sensitive information that they have access to in hard form when it is not in use. If you have access to this information, compliance regulations likely require it. |

## Focus Area 09 - Systems & Application Development

Systems and application development is an area where Information Security needs are often overlooked. The perceived need to get systems up and running quickly sometimes supersedes the need to consider security requirements. Controls are needed for information technology systems to ensure confidentiality, integrity and non-repudiation of your organization’s sensitive information. This section reviews the protection and verification procedures needed for all systems and applications.

Your Information Security Program should include at least the following:

* Specification of security requirements for applications and systems
* Validation of input and output data
* Establishment of a cryptographic control policy
* Protection of system test data, program source code and operational software
* Prevention of information leakage
* Control of outsourced software development
* Properly addressing technical vulnerabilities and updates

|  |  |
| --- | --- |
| **Risk Level:** | Medium - Review as Necessary |
| **Your Score:** | 80% |
| **Recommendations:** | * Consider formalizing testing procedures to ensure that systems are running properly after making changes. |

## Focus Area 10 - Incident Response

Incidents happen, even to the best organizations. Organizations that are prepared to respond when incidents occur respond faster, with fewer financial losses and with less damage to their brand integrity and reputation. Formal procedures should be established for handling information security events. This section covers the basics needed regarding incidents from prevention to lessons learned.

Your Information Security Program should include at least the following:

* Establishment of procedures for reporting information security events and security weaknesses
* Establishment of incident response procedures
* Ensuring that evidence is collected properly
* Ensuring that lessons are learned from information security incidents

|  |  |
| --- | --- |
| **Risk Level:** | High - Immediate Attention Needed |
| **Your Score:** | 20% |
| **Recommendations:** | * Consider formalizing your Incident Response Plan, and testing it with your employees as appropriate. |

## Focus Area 11 - Business Continuity Management

Planning for business continuity in the event of any disruption is vital to an organization. While most organizations have an existing framework for handling business interruptions, this section addresses specifically including and maintaining information security into that process.

Your Information Security Program should include at least the following:

* Inclusion of information security in the business continuity planning process
* Establishment of a common business continuity framework
* Implementation of business continuity plans
* Testing, maintaining, and regular reassessment of the business continuity plans

|  |  |
| --- | --- |
| **Risk Level:** | High - Immediate Attention Needed |
| **Your Score:** | 20% |
| **Recommendations:** | * Consider formalizing your organization's business continuity/disaster recovery plans. Experience has shown that a little time spent in planning upfront saves a lot of headache and expense later |

## Focus Area 12 - Program Maintenance & Compliance

Once an Information Security Policy Program is established, ensuring it remains relevant is essential. This section describes necessary maintenance of the program including legal requirements, upgraded standards and audit considerations.

Your Information Security Program should include at least the following:

* Identification of applicable legislation and regulatory requirements
* Recognition of intellectual property rights
* Protection of organizational records
* Protection of Personally Identifiable Information and Non-Public Information
* Compliance with cryptographic regulations
* Establishment of audit procedures for information systems and the protection of system audit tools

|  |  |
| --- | --- |
| **Risk Level:** | Medium - Review as Necessary |
| **Your Score:** | 73% |
| **Recommendations:** | * Address encryption requirements from an organizational perspective. Ensure that any sensitive information stored on the organization's computing resources is appropriately protected by encryption. |

# Compliance

## Gramm-Leach-Bliley Act

**Compliance Requirement:**  **Required**

The Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act repealed part of the Glass-Steagall Act of 1933. This law provided an opening for investment banks, commercial banks, securities firms and insurance companies to consolidate.

From an Information Security perspective, two key rules under the Act make it significant. First the Financial Privacy Rule puts restrictions in place governing the collection and distribution of a customer’s personal financial information. This applies to both financial institutions, creditors and any company that receives such information. Second, the Safeguards Rule requires that affected organizations much design, implement and maintain appropriate safeguards to protect customer information. The Safeguards rule applies to both financial institutions that collect information from their customers, but also to institutions that receive customer information from other institutions.

***Requirements:***

### Financial Privacy Rule

1. Provide each customer with a privacy notice at the time a consumer relationship is established
2. Provide a privacy notice to each customer on an annual basis
3. Establish a means by which the consumer may opt out of their information being shared with unaffiliated parties
4. Notify consumers anytime there is a change to the privacy policy

### Safeguards Rule

1. Assign an employee to oversee the safeguards
2. Perform a thorough risk assessment on any business operation that handles nonpublic information
3. Develop a program, monitor and test the program to secure information
4. Update the program as necessary as changes are made to how information is collected, stored or used

## Red Flags Rule

**Compliance Requirement: Required**

The Red Flags Rule was implemented by joint Federal Agencies to help affected organizations effectively implement parts 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. These rules are designed to keep organizations from becoming victims of identity theft through doing business unwittingly with identity thieves. The Rule went into effect on January 1, 2008 and is currently slated to begin being enforced on June 1, 2010.

Under part 114, the Rule requires that each financial institution or creditor must develop and implement a written Identity Theft Prevention Program to detect, prevent and mitigate identity theft. This program must look for “red flags” as indicators of identity theft as a part of opening new accounts and maintaining existing accounts

Under part 315, the Rule provides guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

***Requirements:***

The Red Flags Rule requires at least the following:

1. Development and Implementation of a written Identity Theft Prevention Program
2. Controls to prevent and mitigate the risks associated with Identity Theft
3. The Program must be administered by the board of directors or in the case of smaller organizations a member of senior management
4. A compliance report must be delivered on at least an annual basis
5. The Program must be updated periodically
6. The Program must contain an incident response capability
7. The Program must ensure that vendors and suppliers with whom information is exchanged handle the information with procedures that are at least equivalent to the organization’s

## Health Insurance Portability and Accountability Act

**Compliance Requirement: Required**

The Health Insurance Portability and Accountability Act of 1996 was enacted by Congress with two parts. First, Title I protects the health insurance coverage of workers when they lose or change their jobs. Title II of HIPAA established standards for electronic healthcare transactions and national identifiers for employers, health insurance plans and providers.

Title II, often referred to as the Administrative Simplification provisions also addressed both the security and privacy of health related data. The Privacy Rule took effect for most providers on April 14, 2003 with one year extensions for certain small plans. It regulates the use and disclosure of Protected Health Information by covered entities. The Security Rule took effect on April 21, 2003 and required compliance by April 21, 2005 for most entities with a one year extension for certain small plans. The Rule deals specifically with Electronic Protected Health Information and requires administrative, technical and physical safeguards for protecting this information

On November 30, 2009 the Health Information Technology for Economic and Clinical Health Act (HITECH Act) extended the Privacy and Security provisions of HIPAA to business associates of covered entities. This extension also extended the civil and criminal penalties associated with non-compliance to business associates.

***Requirements:***

### Privacy Rule

1. Requires the disclosure of PHI data to the patient within 30 days of request
2. Requires authorization to provide PHI data to other providers, notwithstanding legal burden
3. Entity must make reasonable efforts to disclose only the minimum PHI required
4. Requires that individuals be able to correct inaccurate PHI
5. Requires entities to implement measures ensuring that patient communication remains confidential

### Security Rule

1. Administrative Safeguards – primarily written policies and procedures designed to clearly express how the organization will comply with the Act. Policies must be overseen by management and updated periodically
2. Physical Safeguards – express how physical access to PHI data will be controlled. Also covers how PHI data will be disposed of properly
3. Technical Safeguards – ensure that network and computer systems used to store and transport PHI data are hardened to keep anyone other than the intended recipient from accessing the information

### HITECH Act

1. Requires entities that have lost PHI data to report the breach and notify affected victims

## Payment Card Industry Data Security Standard

**Compliance Requirement: Required**

The Payment Card Industry Data Security Standard (PCIDSS, PCI) was created by the Payment Card Industry Security Standards Council made up of the major credit card providers in an effort to prevent fraud through identity theft and unauthorized card use.

Any merchant who accepts credit cards is required to comply with some form of the standard as a provision of their contract with their merchant provider. Compliance must be assessed on an annual basis. Depending on the size, complexity and number of transactions processed, this assessment may be performed either internally or through an external provider.

### Requirements:

1. Installation and maintenance of a firewall
2. All vendor supplied passwords and default passwords must be changed
3. Cardholder data must be protected by appropriate controls
4. All transmission of cardholder data across public or open networks must be encrypted
5. Antivirus software must be in use on all systems
6. All applications and systems must be appropriately secure
7. Access to cardholder data must be on a need-to-know basis
8. Each computer user must be assigned a unique user ID and password
9. Physical access to cardholder data must be restricted
10. Any access to cardholder data must be monitored and tracked
11. Security systems and controls must be tested on a regular basis
12. The organization must maintain an Information Security Policy

## Federal Information Security Management Act

**Compliance Requirement: Not Required**

The Federal Information Security Act of 2002 (FISMA) was enacted at Title III of the E-Government Act of 2002. The act recognizes the importance of Information Security to both the national security and the economic security of the nation. As such, it requires every federal agency, and any contractor or third party who manages or supports assets of the agency to implement an Information Security Program.

As outlined by the National Institute of Standards and Technology (NIST) in publication NIST SP 800-18, a framework has been developed to ensure that each agency is able to cost effectively reduce the information security risks that it faces.

Requirements:

1. Inventory of information systems operated or under the control of the agency
2. Information systems and information must be categorized by risk level as outlined by NIST SP 800-60
3. Appropriate security controls must be applied to information systems as outlined by FIPS 200 (Minimum Information Security Requirements for Federal Information and Information Systems)
4. A risk assessment must be performed to identify additional controls that may be necessary.
5. Development and maintenance of a System Security Plan (Information Security Program)
6. Programs must be certified and accredited as defined by NIST SP 800-37

## Family Educational Rights and Privacy Act

**Compliance Requirement: Not Required**

The Family Educational Rights and Privacy Act of 1974 (FERPA), also sometimes known as the Buckley Amendment regulates how educational institutions and other agencies who receive funding from the United States Department of Education provide students with access to their educational records. The law also regulates how students may seek to have their records amended, as well as giving the student some control over how their information is disclosed.

The law states that with a few exceptions, the school or agency must have a student’s permission before their records are disclosed.

The law also regulates how state agencies protect privacy of information in transmitting testing information to federal agencies.

While the law has classically allowed schools to share information about students if there is a “health or safety emergency”, the definition of emergency has been defined narrowly. The law was revised in December 2008 as it applies to mental health and campus safety issues allowing for the disclosure of information in situations where there is an “articulable” and significant threat to either the student or other individuals.

Requirements:

1. Students have the right to access educational records kept by the school
2. Students may demand that their records only be disclosed with their consent
3. Students may amend or correct their educational records as appropriate
4. Directory information may be released without prior consent, however the student has the right to restrict the disclosure of their directory information
5. Non-directory Information (SSN, race, nationality, gender, transcripts, etc…) may only be disclosed with a student’s prior written consent. This includes disclosure to parents.
6. FERPA Policies must be updated on an annual basis
7. FERPA Policies must be communicated to students on an annual basis

# Next Steps

Thank you again for taking the time to complete this Needs Assessment.

If you are like most of the organizations that we work with, you’ve just finished reading this report and have some major questions about where to go from here. Rest assured that Net Reaction has helped thousands of organizations understand their Information Security Needs, and is committed to helping you understand your organization’s specific needs.

Every organization is different, and each has areas in which they can improve. We have highlighted some of those areas for your organization in this report. We would be happy to discuss them with you further, and invite you to give us a call at your convenience to speak about your path forward from here.