CommunityIT Innovators®
where technology meets mission

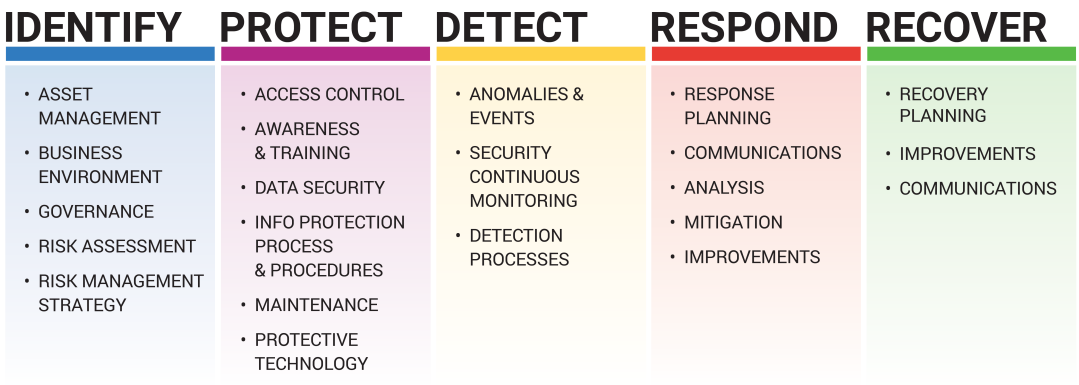
NIST Security Risk Assessment

Risk Assessment Report
Completed On: 25 May 2019

Thank you for taking the time to respond to this NIST Security Risk Assessment. The goal of this assessment is to arrive at a quick sense of your strengths and weaknesses, and to provide advice as to what improvements you should be considering.

Your results have been measured against the National Institute of Standards and Technology (NIST) model regarding their cybersecurity for small business. This standard is referred to as the NIST Cybersecurity Framework (NIST CSF) and is considered a best practice in the Security Industry.

The Standard measures five key areas to help you in understanding and safeguarding critical business information.



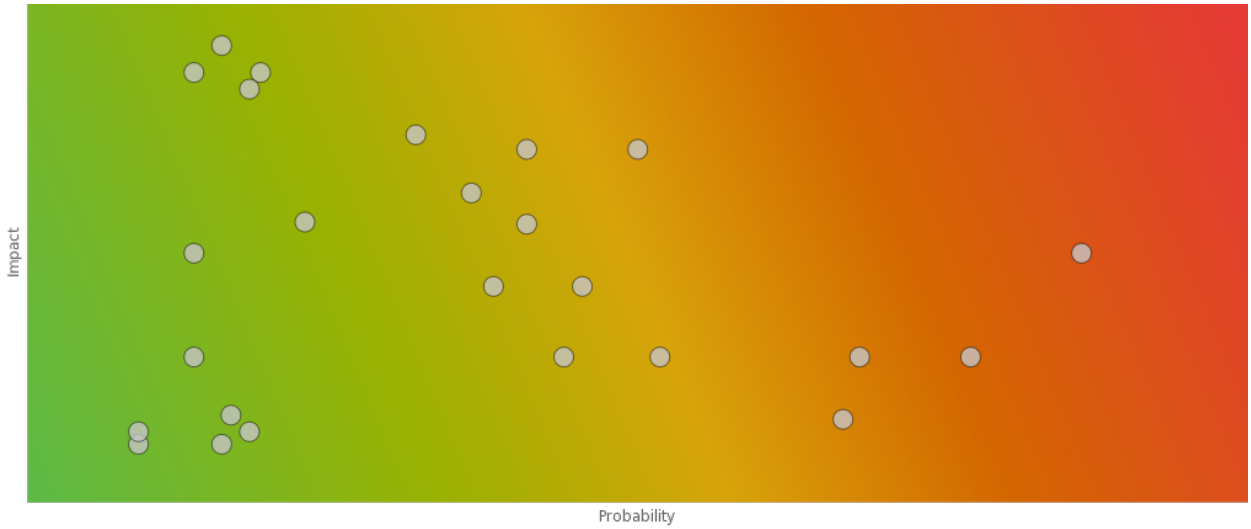
Your results will be measured against those of similar size as a metric of where your security practices align to the framework. The following link will take you directly to the NIST site where you can download the document for your own reference:

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

OVERALL RISK ASSESSMENT

Your overall risk rating is **MEDIUM**

Your overall rating for this assessment raises some concerns as to your ability to detect and prevent threats that would negatively impact your organization. You should pay careful attention to the recommendations and remediate as many of the high risk items as you can.



TOP RISK AREAS

Critical	PR.AT-1 - All users are informed and trained
Critical	ID.RA-3 - Threats, both internal and external, are identified and documented
High	ID.RA-1 - Asset vulnerabilities are identified and documented
High	DE.CM-3 - Personnel activity is monitored to detect potential cybersecurity events
High	ID.RA-2 - Threat and vulnerability information is received from information sharing forums and sources

TOP RISK AREA RECOMMENDATIONS

PR.AT-1: All users are informed and trained — Critical

Q: Do you require Information Security training for your employees?

A: No

Importance:
It is essential to your business to ensure your employees are trained on the constantly changing security threats and how to avoid these threats.

Remediation Steps:
There are several on-line security awareness training companies and sign your employees up for annual security awareness training.

ID.RA-3: Threats, both internal and external, are identified and documented — Critical

Q: Are potential impacts from third parties identified and documented?

A: No

Importance:
Some of the largest data breaches to date have come as a result of a third-party contractors inability to protect their environment. Practices should be in place to ensure you know your risk of doing business with external entities.

Remediation Steps:
You should immediately create an inventory of your vendors, review your contracts for obligations to protect your data, and perform a risk assessment across your inventory so that you can determine the risks to your business.

ID.RA-1: Asset vulnerabilities are identified and documented — High

Q: Does your organization have an internal process for assessing risk?

A: No

Importance:
Along with having security policies, a risk assessment is the most fundamental element to protecting your vital business assets. By not having one performed you are essentially blind to the risks and severity of the risks that can impact your business.

Remediation Steps:
Create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

High

Q: Are you using an email filtering solution?

A: No

Importance:
Malware and other malicious software is most often spread through email. Unfiltered enterprise emails can be frustrating for both the administrators and your users.

Remediation Steps:
You should add an email filtering tool to your environment. The spam blocker or filter prevents unwanted emails from reaching your inbox and prevents any consequential harm to your business.

Q: Do you have web filtering or web site blocking set up?

A: No

Importance:
By not having web filtering you allow your employees to go to web sites which can potentially contain malicious software which can be downloaded and infect your environment.

Remediation Steps:
Implement a web filtering tool in your environment. Web filtering delivers many positive benefits for both organizations and end-users that go far beyond the basic implementation of preventing access to named websites or particular types of websites. The benefits and capabilities of web filtering are productivity, minimize liability, network and bandwidth management and data security.

ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources

High

Q: Do you receive threat intelligence information from sharing sources such as ISACs?

A: No

Importance:

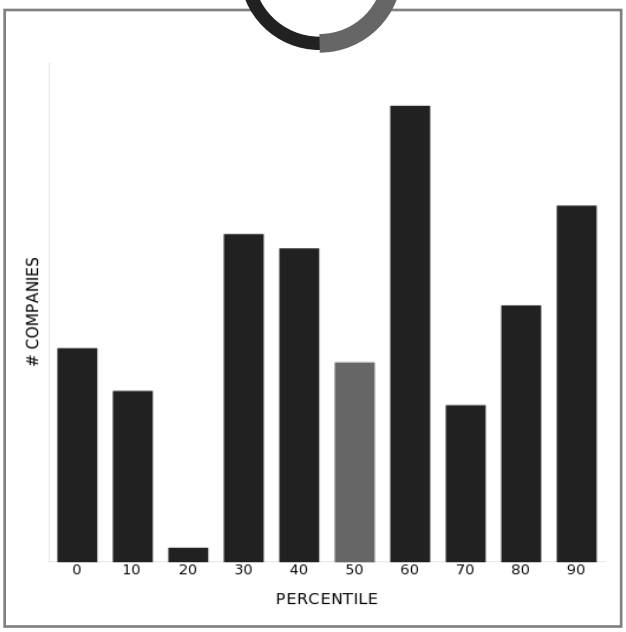
Leveraging Threat intelligence is important as you can gain vital information about your business sector that would enable you to detect and defend against known attacks. You should find out for sure if you are receiving this important information. Not having this information is a significant gap.

Remediation Steps:

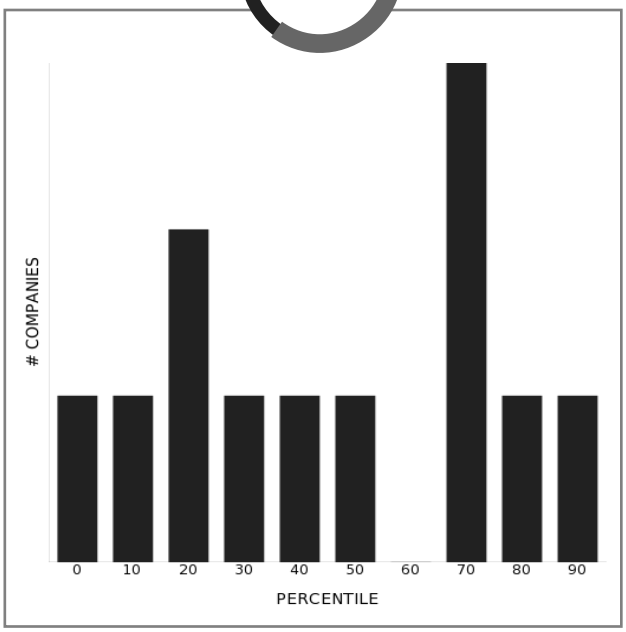
Check with your security team to see if you are receiving threat intelligence information. If you are not receiving this information seek out an ISAC that aligns to your business model and leverage the available tools on the market to enable a threat intelligence capability for your company.

INDUSTRY COMPARISONS

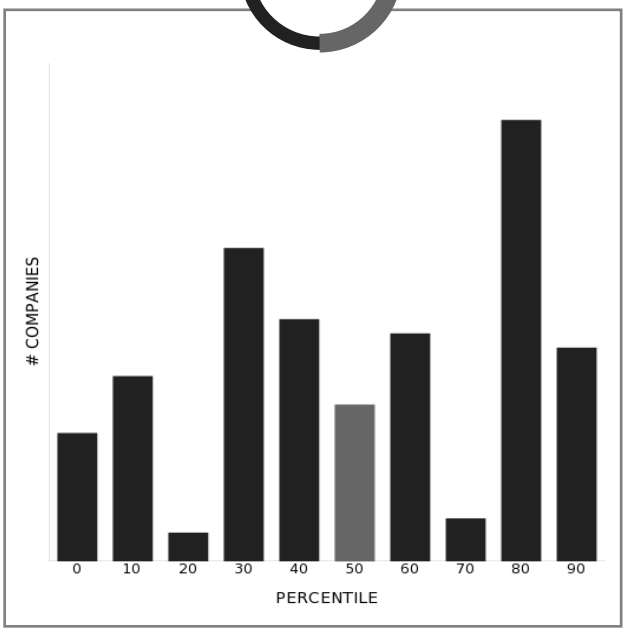
OVERALL 50TH PERCENTILE



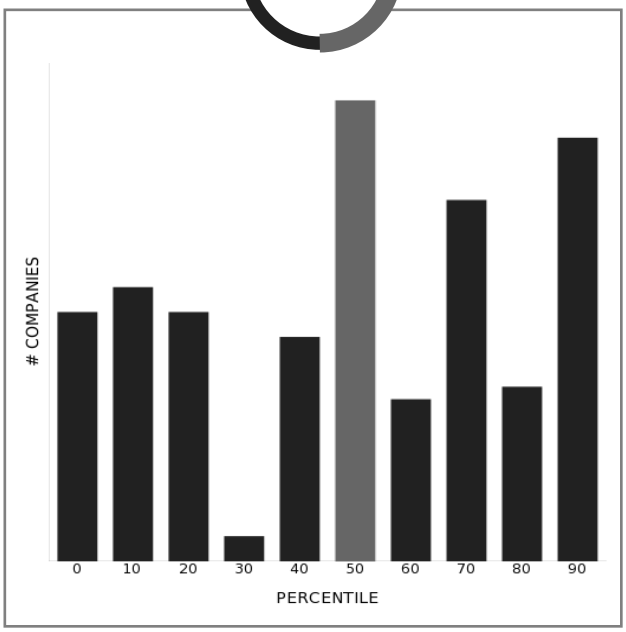
INDUSTRY 60TH PERCENTILE



COMPANY SIZE 50TH PERCENTILE



LOCATION 50TH PERCENTILE



APPENDIX / QUESTIONS

Q: Please enter your name.

A: Matthew Eshleman

Q: Please enter your company name.

A: Sample Company

Q: Please enter your role in the organization.

A: Office Manager

Q: Please select the industry of the company.

A: Not for Profit

Q: Please select the number of employees in the company.

A: 1-500

Q: Where are you located?

A: United States

Q: Please enter your email address.

A: meshleman@gmail.com

Q: What best describes your annual revenue?

A: Not for Profit

Q: Who manages your IT environment? (Choose all that apply)

A: MSP/IT
Your digital workplace environment is vulnerable if managed by untrained individuals.

APPENDIX / QUESTIONS

Remediation Steps:
Having your digital workplace managed by trained individuals is preferred.

Q: Who has access to your computer hardware? (Choose all that apply)

A: MSP/IT
Restricting device access to authorized users is the way to go.

Remediation Steps:
Only those users who have been authorized access with a legitimate business purpose should have access to your computer hardware.

Q: Do you have a listing of all user accounts?

A: Yes

Q: Do any of your users have admin access?

A: I don't know
You should always have knowledge of the users in your company that have administrative access to your IT assets.

Remediation Steps:
Ensure that you know whether an inventory exists, or if not create one.

Q: Do you have an inventory of devices such as printers, computers and scanners for your business?

A: Yes
Important business information as well as sensitive personal information could be stored on your IT devices. If you do not have an accurate inventory then these devices could be leveraged by people outside of your company for personal gain and damage to your business.

Remediation Steps:
Depending on the size of the organization and the number of devices, an automated inventory application may make it easier to keep track of changes assuming the current inventory is being done manually.

APPENDIX / QUESTIONS

Q: Is your physical office locked when vacant?

A: Yes

Not having the ability to physically secure your office is the same as leaving your home unlocked. Valuable assets and information can be stolen which can tarnish your reputation and impact your business potential

Remediation Steps:

This is good news. A locked office is a good deterrent.

Q: How long before your computer screen is set to lock when not in use anytime you're away from your computer?

A: Never

Leaving your computer unlocked while you are away from it allows other employees or non-employees access to your business information.

Remediation Steps:

Implement an auto-lock feature for a set period of time no more than 15 minutes, or get into the practice of locking it manually consistent with the operating system that you are using.

Q: Do you perform background checks on your employees?

A: Yes

Q: How are background checks performed?

A: Upon new hire and annually thereafter

Q: Are user credentials shared?

A: No

User credentials should never be shared even if you are in a small office environment. Determining accountability for actions is near impossible when credentials are shared

Remediation Steps:

This is a good practice. Sharing user credentials not only limits the ability to successfully audit activities, it also prevents knowing if a user's credentials have been compromised.

APPENDIX / QUESTIONS

Q: Does your company have information security policies and procedures?

A: No

Security policies are the guidelines that indicate managementís intentions on securing their physical and information assets. They also provide guidance on acceptable use of these assets and the ramifications should they not be followed.

Remediation Steps:

Security policies are often tied to security frameworks and can be purchased online or created by a consultant or MSP. This is a foundational element that is a must have for your company

Q: Does your organization have an internal process for assessing risk?

A: No

Along with having security policies, a risk assessment is the most fundamental element to protecting your vital business assets. By not having one performed you are essentially blind to the risks and severity of the risks that can impact your business.

Remediation Steps:

Create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.

Q: Do you receive threat intelligence information from sharing sources such as ISACs?

A: No

Leveraging Threat intelligence is important as you can gain vital information about your business sector that would enable you to detect and defend against known attacks. You should find out for sure if you are receiving this important information. Not having this information is a significant gap.

Remediation Steps:

Check with your security team to see if you are receiving threat intelligence information. If you are not receiving this information seek out an ISAC that aligns to your business model and leverage the available tools on the market to enable a threat intelligence capability for your company.

Q: Are potential impacts from third parties identified and documented?

A: No

APPENDIX / QUESTIONS

Some of the largest data breaches to date have come as a result of a third-party contractors inability to protect their environment. Practices should be in place to ensure you know your risk of doing business with external entities.

Remediation Steps:
You should immediately create an inventory of your vendors, review your contracts for obligations to protect your data, and perform a risk assessment across your inventory so that you can determine the risks to your business.

Q: Do you limit access to data for your employees?

A: Yes, employees only have access to data for their job role
Limiting access to data may prevent an accidental or intentional loss of sensitive information from your organization.

Remediation Steps:
Ensure the organization is reviewing this access on a regular basis.

Q: After termination, do you disable accounts?

A: Yes
Disabling accounts immediately upon termination is a best security practice to prevent access to the organization upon termination.

Remediation Steps:
Disabling accounts immediately upon termination is a best security practice to prevent access to the organization upon termination.

Q: How long after termination do you disable user accounts?

A: Within 24 hours
User accounts of employees who are terminated or resign should be disabled immediately, waiting up to a week as you noted is too long. Work on a procedure to disable those accounts in a more timely manner.

Remediation Steps:
This is a good practice. Disabling terminated users within 24 hours ensures the user is unable to access the organization, even from a remote location.

APPENDIX / QUESTIONS

Q: Do you allow the use of USB ports?

A: No
USB ports on portable computers should be disabled, if they will not be used.

Remediation Steps:
Disable any USB ports on portable devices.

Q: Do you provide surge protection to your computer systems?

A: Yes

Q: Do you keep up with the latest Critical Updates and Microsoft Windows updates?

A: Yes
You keep up with the latest critical updates and Microsoft Windows patches.

Q: How are the updates completed?

A: Auto Updates
It is important to make sure that patches are installed in the timeframe that the policy specifies.

Remediation Steps:
Updates are installed automatically and users are notified to reboot their computers so that the patch is applied.

Q: Are all your software applications still supported by the manufacturer?

A: Yes
You make sure that software applications are still supported by the manufacturer.

Remediation Steps:
Currently used software applications are still supported by the manufacturer.

Q: Do you keep software licensing agreements up to date?

A: Yes
Software agreements are kept up to date.

APPENDIX / QUESTIONS

Remediation Steps:
Software licenses are checked and agreements are kept up to date.

Q: Are you using a firewall between your internal network and the internet?

A: Yes
Firewalls should be set with a "DENY ALL" for all inbound traffic at a minimum. With very few exception, nothing from the outside should be allowed into the network without first originating in the network.

Remediation Steps:
Ensure the firewall rules are properly setup to block unwanted traffic and that logging is enabled for all rules so the organization can audit for any unwanted traffic that may still be allowed. Ensure only authorized personnel have the ability to access and make changes to the organization's firewall.

Q: Who configures and manages your firewall? (Choose all that apply)

A: MSP/IT consultant
Trained individuals are less likely to make a mistake configuring the firewall.

Remediation Steps:
Ensure the MSP/IT individual is reviewing the firewall logs and the firewall rules on a regular basis to ensure unwanted traffic is not able to gain access to the environment.

Q: Have you changed the default password for your firewall?

A: Yes
Not changing the default password on your wireless access device can lead to a possible compromise of your system and critical information you are storing. This is possible because others know what the default passwords are and can access your system.

Q: Is your firewall set to log activity?

A: No

APPENDIX / QUESTIONS

Your firewall is designed to keep track of events such as failed login attempts, and events relating to the firewall rules that give you an indication if the rules are working or if you need additional items that are specific to your network. Not having this enabled means you do not have any insight as to the types of traffic or access attempts which can be harmful if your firewall is not properly configured

Remediation Steps:
You should configure your firewall to log activity as soon as you can and establish a process to read the logs at reasonable intervals. Doing so can help you make valuable adjustments to your firewall settings.

Q: Are you using WiFi for your business?

A: Yes
Wireless networks can be an access gateway for unwanted network traffic. Ensure your wireless is properly configured to prevent unauthorized access to your network.

Remediation Steps:
Ensure your wireless is properly configured to prevent unauthorized access. This includes the passphrase and the encryption algorithm. If possible, authentication to LDAP or RADIUS is preferred.

Q: Which authentication method do you use on your router?

A: No password
Not having an authentication method established means that anyone can see and connect to your wireless device. This not only affects the security of your allowed devices, but also enables people that you do not know to consume network access without your knowledge or approval.

Remediation Steps:
Enable WPA2 or RADIUS. If you are unsure how to do this, please contact your MSP, ISP, or an IT Security consultant.

Q: Have you changed the default administrative password on your wireless access device?

A: Yes
Changing the default password is paramount to good security.

Remediation Steps:

APPENDIX / QUESTIONS

Good job. In addition to simply changing the default password, it should also be a very strong complex password to ensure maximum difficulty in attempting to crack it.

Q: How do you store/ protect the wireless access device password?

A: Remembered by one person
It's risky having a person remember your WiFi admin password. If they forget it you will have to reset your router to the default setting and lose any configurations you have made.

Remediation Steps:
There are password managers which give you the option to sync to multiple devices or keep them local only. Consider switching to one of these password managers instead of trying to remember all your passwords.

Q: Do you scan your environment for rogue access points?

A: No
Having access points within your environment which you don't know about can lead to vital business assess being stolen without your knowledge.

Remediation Steps:
You should scan your environment for rogue access points and remove them from your network.

Q: Are you using an email filtering solution?

A: No
Malware and other malicious software is most often spread through email. Unfiltered enterprise emails can be frustrating for both the administrators and your users.

Remediation Steps:
You should add an email filtering tool to your environment. The spam blocker or filter prevents unwanted emails from reaching your inbox and prevents any consequential harm to your business.

Q: Do you have web filtering or web site blocking set up?

A: No

APPENDIX / QUESTIONS

By not having web filtering you allow your employees to go to web sites which can potentially contain malicious software which can be downloaded and infect your environment.

Remediation Steps:
Implement a web filtering tool in your environment. Web filtering delivers many positive benefits for both organizations and end-users that go far beyond the basic implementation of preventing access to named websites or particular types of websites. The benefits and capabilities of web filtering are productivity, minimize liability, network and bandwidth management and data security.

Q: How are old equipment and data storage devices handled before disposal?

A: Data is removed from hard disks, devices and removable meda before being disposed.
You are managing end of life to limit your security exposure.

Q: How are hard copy documents handled before disposal?

A: Documents are shredded and disposed of by a third-party vendor
You properly dispose of your hard copy documents.

Remediation Steps:
Documents are shredded and disposed of by a third-party vendor.

Q: Do you require Information Security training for your employees?

A: No
It is essential to your business to ensure your employees are trained on the constantly changing security threats and how to avoid these threats.

Remediation Steps:
There are several on-line security awareness training companies and sign your employees up for annual security awareness training.

Q: Do you have a threat detection product in place today?

A: Yes
You have threat detection today.

APPENDIX / QUESTIONS

Remediation Steps:
You have threat detection today.

Q: How are you handling threat information today? (Choose all that apply)

A: Detected events are analyzed
You are collecting, detecting and analyzing security events.

Remediation Steps:
You are collecting, detecting and analyzing security events.

Q: Are you monitoring your IT environment for anomalous events?

A: Yes
You have an anomalous event monitoring solution.

Remediation Steps:
You have an anomalous event monitoring solution.

Q: Which of the following are you monitoring for cybersecurity events? (Choose all that apply)

A: The network is monitored to detect potential cybersecurity events

Q: What other types of activity is your security monitoring looking for? (Choose all that apply)

A: Malicious Code

A: External Service Providers activity

A: Connections

A: Software

Q: Do you perform vulnerability scans in your environment?

A: No
Not performing vulnerability scans in your environment can lead to undetected threats which can be exploited within your environment.

Remediation Steps:

APPENDIX / QUESTIONS

Purchase a vulnerability scanning tool to implement regular vulnerability scans of your environment. Consider doing third-party vulnerability scans on a yearly basis.

Q: Do you have incident response processes and procedures in place which are being maintained on a regular basis?

A: No

It is critical to businesses ability to respond to and recover from a security event and you don't have a plan to do so.

Remediation Steps:

Create a business continuity and disaster recovery plan for your business. Work with a security consulting firm if you need assistance creating these plans.

Q: Are you planning on developing incident response processes and procedures?

A: Yes

Q: What is the time frame you are looking at to develop incident response processes and procedures?

A: Within a Year

Having response processes and procedures to ensure your business can continue to run after a recovery is needed is critical.

Remediation Steps:

You should consider moving your plan to create recovery processes and procedures up in priority and complete within the next six months. There are professional services available who can assist you with this process.

Q: Are recovery processes and procedures documented and reviewed?

A: Yes, reviewed annually.

Q: Are recovery processes and procedures tested?

A: Yes

APPENDIX / QUESTIONS

Q: When was the last time recovery processes and procedures were tested?

A: In the last six months

Q: Do you incorporate lessons learned into your recovery planning and processes?

A: Yes

Q: Do you have a communication plan in place to coordinate restoration activities with internal and external parties?

A: No

The time to create a communications plan is before you actually need one. These plans need to be well thought out and reviewed thoroughly before they are implemented.

Remediation Steps:

You need to create a communications plan. To do that research sites such as SANS.org or DRI International and look for Incident Response, Disaster Recovery, and Business Continuity. These sites will likely have templates that can be downloaded and modified for your business

ATTESTATION LETTER

Customer Name: Sample Org ("Customer")
Managed Service Provider: Community IT ("MSP")

Date: _____

The above-named MSP has recommended a specific course of action to the Customer to help improve the Customer's overall security posture (the "Report") and the Customer acknowledges it has been provided and has reviewed the Report. The Report provides a prioritized description of the risks to the Customer as aligned with the NIST Cybersecurity Framework (NIST CSF), which is considered a best-practices approach to follow. The recommendations contained within the Report represent the Customer's best interests and requires careful consideration.

The specific recommendation(s) being made by the MSP include the following:

_____

_____

_____

Given that the Customer has elected not to follow the recommendations of the MSP as noted above and as outlined within the Report, the Customer accepts the risks outlined in the Report and releases the MSP from any responsibility resulting from incidents related to such risks. The risks of not following the recommendations of the MSP have been fully explained to the Customer by the MSP. The Customer agrees that the MSP shall not be held responsible or legally liable for the decision or any future consequences of the Customer's decision.

By signing below the Customer acknowledges that it has read this information and has elected not to follow the MSP's recommendations.

AGREED AND ACCEPTED:

SAMPLE ORG

BY: _____

ITS: _____

DATE: _____