ConnectWise Identify®

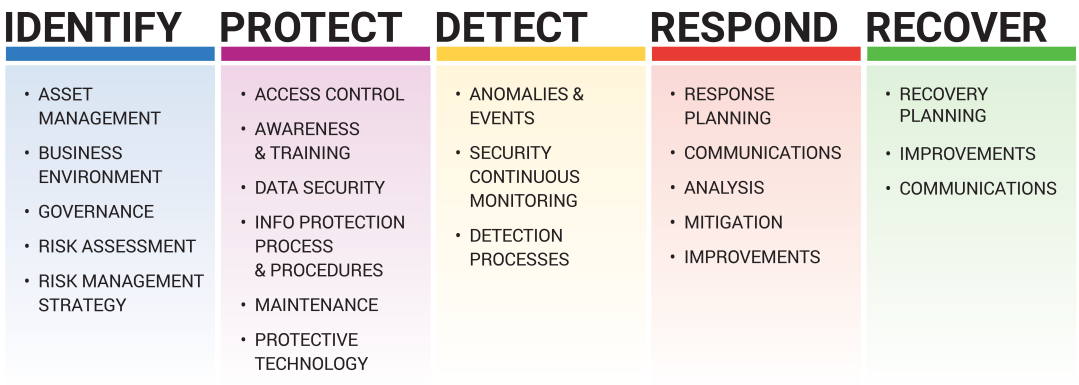
ThirstyDesign, L.L.C.

Risk Assessment Report
Completed On: 23 Apr 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.



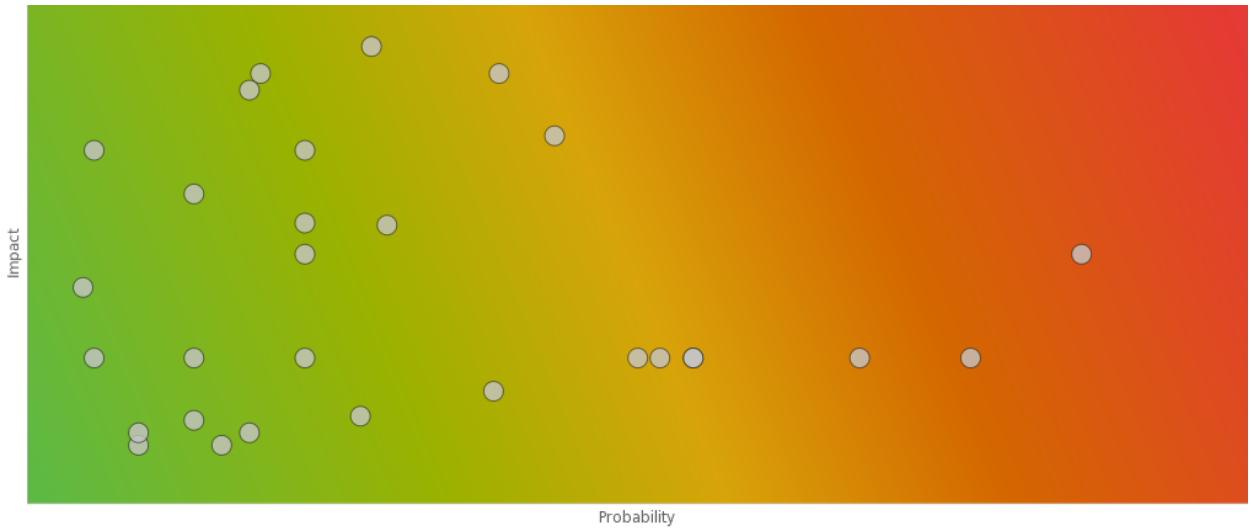
Your results will be measured against those of similar size as a metric of where your security practices align to the framework. The following link will take you directly to the NIST site where you can download the document for your own reference:

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

OVERALL RISK ASSESSMENT

Your overall risk rating is **LOW**

Congratulations! Your overall risk determined from the assessment conveys a diligence on your part to ensure you are doing what is needed to maintain the security of your organization.



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	RS.IM-1 - Response plans incorporate lessons learned
High	RS.RP-1 - Response plan is executed during or after an event
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: I'm not sure

Importance:
You should know whether your firm performs periodic risk assessments so you can have knowledge of and plan for the remediation of those risks.

Remediation Steps:
Work with your company leaders to determine of you have performed a risk assessment and if not then you should create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.

RS.IM-1: Response plans incorporate lessons learned

High

Q: Do you conduct an analysis of your incident response and support recovery activities to ensure they are adequate?

A: No

Importance:
Businesses change over time and so do their capabilities to response and recover from a security incident.

Remediation Steps:
Analyze and update your response and recovery plans on at least an annual basis.

Q: Do you improve organizational response activities by incorporating lessons learned from security incidents?

A: No

Importance:
You are not incorporating lessons learned from a security incident or test of your response plan. This is needed to ensure you can better respond to similar incidents in the future.

Remediation Steps:
Go back to your last security incident or test of your response plan and document the lessons you learned from this event. Update your response and recovery plans with this information.

RS.RP-1: Response plan is executed during or after an event

High

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

A: Yes, reviewed as needed

Importance:
Response processes and procedures need to be reviewed at least annually.

Remediation Steps:
Establish a policy to review all your information security policies and procedures at least annually.

Q: Are incident response processes and procedures tested?

A: No

Importance:
Without testing your response processes and procedures you don't know for sure you will be able to recover your systems and data in the event of a security incident.

Remediation Steps:
You should implement a test plan and execute it at least once. The time to test an IR plan is not during an incident.

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?

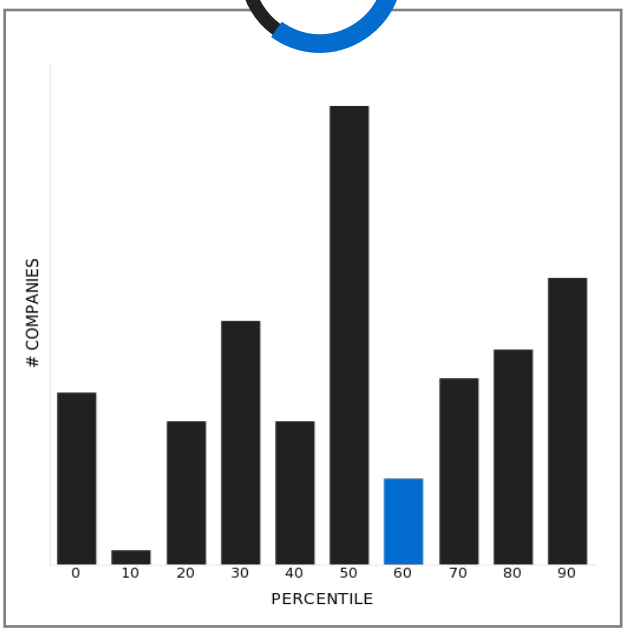
A: No

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.

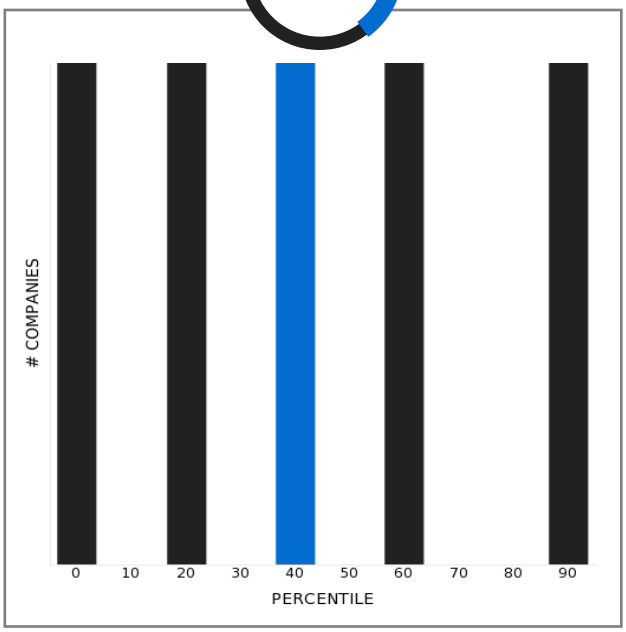
Remediation Steps:
Check with your security team to see if you are receiving threat intelligence information. If you are not receiving this information seek out an ISAC that aligns to your business model and leverage the available tools on the market to enable a threat intelligence capability for your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

INDUSTRY COMPARISONS

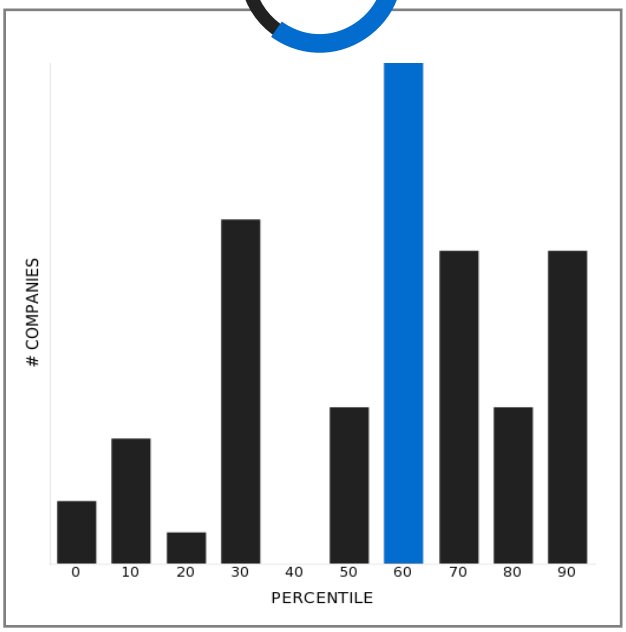
OVERALL 60TH PERCENTILE



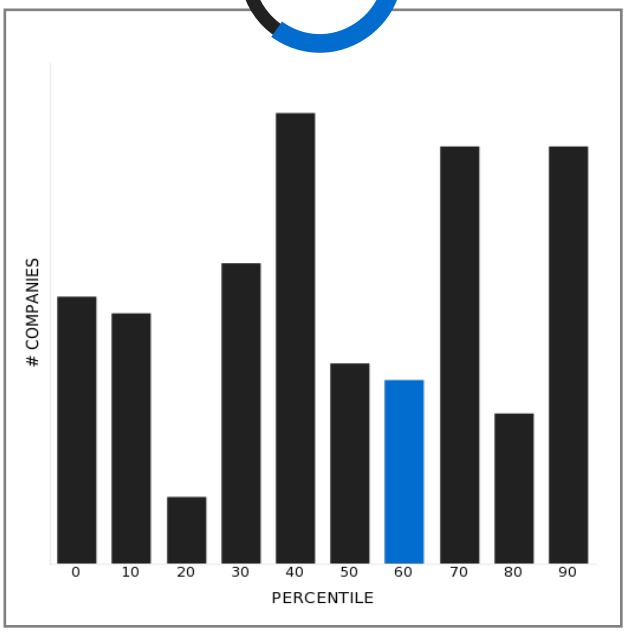
INDUSTRY 40TH PERCENTILE



COMPANY SIZE 60TH PERCENTILE



LOCATION 60TH PERCENTILE



APPENDIX / QUESTIONS

Q: Please enter your name.

> **A: Bill Walton**

Q: Please enter your company name.

> **A: Thirsty Design**

Q: Please enter your role in the organization.

> **A: President**

Q: Please select the industry of the company.

> **A: Business Services**

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: BillW@thirstydesign.com**

Q: What best describes your annual revenue?

> **A: $1M - $5M**

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: Yes
Admin access allows users to install, delete, or modify applications and programs that may not be consistent with your business model.

Remediation Steps:
Remove admin access, or limit the use of admin access for only those occasions where it is truly needed.

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

A: No
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:
Implement an asset management process/product.

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: Less than 15 minutes
This reduces the likelihood of another individual having the ability to access the device using another user's credentials.

Remediation Steps:
This is a good practice. Best practice is for users to "lock" their computer when they leave their desk.

Q: Do you perform background checks on your employees?

A: Yes

Q: How are background checks performed?

A: Only at new hire
Background checks should be performed on an annual basis as many items that may impact your business through an employees behavior may not be visible to you.

Remediation Steps:
Update your policy, notify your employees, and perform background checks on an annual basis.

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

APPENDIX / QUESTIONS

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.

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

A: Yes

Q: Have your employees been made aware of your information security policies and procedures?

A: Yes
All employees should be aware of the organization's policies and procedures including those for cybersecurity. Your employees are part of the defense. They should be re-trained every year.

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

A: I'm not sure
You should know whether your firm performs periodic risk assessments so you can have knowledge of and plan for the remediation of those risks.

Remediation Steps:
Work with your company leaders to determine of you have performed a risk assessment and if not then you should 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:

APPENDIX / QUESTIONS

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
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 a week

APPENDIX / QUESTIONS

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:
Create a policy and a process to monitor accounts and disable them as soon as possible but not later than 24 hours.

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.

APPENDIX / QUESTIONS

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.

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: Myself
It's ok that you configure your firewall yourself as long as you have the experience to configure permissions for programs and services, connection settings, and log settings.

Remediation Steps:
We highly recommend that you seek guidance from your firewall vendor, MSP, or other qualified security expert to make sure your firewall settings are appropriate for your company.

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

A: Yes

APPENDIX / QUESTIONS

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: Yes
Logging activity on your firewall helps in detecting unwanted network attempts into your environment. Logs will also show successful attempts as well.

Remediation Steps:
Firewall logs should be ingested into a SIEM to aid in detecting unwanted network traffic. Be sure your logs are looking at both inbound and outbound events to determine if you have been breached.

Q: How often are the firewall logs reviewed?

A: Occasionally
Occasional review may be fine so long as that time frame is no longer than a week. Any longer than this and you run the risk of missing vital information. Additionally, some firewall logs have a specific number of logs that it stores before being overwritten, which means you could be missing vital information related to the risks to your environment

Remediation Steps:
We recommend that your firewall logs are reviewed on a weekly basis at the very least.

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: WPA2 personal

APPENDIX / QUESTIONS

WPA2 Personal is better than WEP, using WPA2 Enterprise would be better.

Remediation Steps:
WPA2 Personal is better than WEP, using WPA2 Enterprise would be better.

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:
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: Locked in a secure location such as a password manager or combination safe
Having the password stored in a secure location only accessible by authorized individuals offers the lowest risk.

Remediation Steps:
Ensure the locked location is accessible by all authorized individuals and not by a single individual. Password should be changed on a regular interval defined by the organization as well.

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: Yes

APPENDIX / QUESTIONS

Q: What do you use for email filtering?

> **A: McAfee**

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

> **A: Yes**

Q: What do you use for website filtering and blocking?

> **A: McAfee**

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 in house then thrown away**
> *You properly dispose of your hard copy documents.*
>
> *Remediation Steps:*
> *Documents are shredded in house then thrown away.*

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**

APPENDIX / QUESTIONS

You have threat detection today.

Remediation Steps:
You have threat detection today.

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

A: Incident alert thresholds are established
Undetected events that are not collected, analyzed, investigated and remediated can cause risk to your company.

Remediation Steps:
Events that are collected should be analyzed, investigated and remediated.

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

A: No
Not being able to monitor and detect threats in your IT environment can lead to unnecessary downtime or security incidents.

Remediation Steps:
Implement a monitoring solution for detect and alert on anomalous behavior in your environment.

Q: Do you perform vulnerability scans in your environment?

A: Yes

Q: How often are vulnerability scans performed?

A: Monthly

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

A: Yes, reviewed as needed
Response processes and procedures need to be reviewed at least annually.

Remediation Steps:

APPENDIX / QUESTIONS

> *Establish a policy to review all your information security policies and procedures at least annually.*

Q: Are incident response processes and procedures tested?

> **A: No**
> *Without testing your response processes and procedures you don't know for sure you will be able to recover your systems and data in the event of a security incident.*
>
> *Remediation Steps:*
> *You should implement a test plan and execute it at least once. The time to test an IR plan is not during an incident.*

Q: If a cybersecurity incident occurred, are you comfortable that your response plans and procedures will enable you to rapidly react to the event?

> **A: I don't know**
> *Your IR Plan should be nimble in nature to allow you to respond quickly to suspected cybersecurity events. This is the reason why they should be tested and analyzed*
>
> *Remediation Steps:*
> *You should schedule a test of your IR Plan and pay careful attention to the timeliness and effectiveness of the plan. Make changes to ensure that you can respond rapidly.*

Q: Which of the following are part of your incident response processes and procedures? (Choose all that apply)

> **A: Personnel know their roles and order of operations when a response is needed**

Q: Do you conduct an analysis of your incident response and support recovery activities to ensure they are adequate?

> **A: No**
> *Businesses change over time and so do their capabilities to response and recover from a security incident.*
>
> *Remediation Steps:*
> *Analyze and update your response and recovery plans on at least an annual basis.*

APPENDIX / QUESTIONS

Q: Which of the following activities are performed to prevent expansion of a cybersecurity event, mitigate its effects, and eradicate the incident?

> **A: Incidents are contained and mitigated**

Q: Do you improve organizational response activities by incorporating lessons learned from security incidents?

> **A: No**
> *You are not incorporating lessons learned from a security incident or test of your response plan. This is needed to ensure you can better respond to similar incidents in the future.*
>
> *Remediation Steps:*
> *Go back to your last security incident or test of your response plan and document the lessons you learned from this event. Update your response and recovery plans with this information.*

Q: Are recovery processes and procedures documented and reviewed?

> **A: Yes, reviewed as needed not necessarily on an annual basis**
> *Businesses change over time and so do their capabilities to respond and recover from a security incident. These processes should be reviewed at least annually and as needed when changes are made.*
>
> *Remediation Steps:*
> *Implement a process to review your recovery processes and procedures annually.*

Q: Are recovery processes and procedures tested?

> **A: Yes**

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

> **A: Between six months and a year**

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

> **A: Yes**

APPENDIX / QUESTIONS

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

> **A: Yes**

Q: Which internal and external parties are part of your communication plan? (Choose all that apply)

> **A: Internet Service Providers (ISPs)**

ATTESTATION LETTER

Customer Name: ThirstyDesign, L.L.C. ("Customer")
Managed Service Provider: Sienna Group CW Testing (spmdj_c) ("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:

THIRSTYDESIGN, L.L.C.

BY: _____

ITS: _____

DATE: _____