ingenio TECHNOLOGIES

Risk Assessment Report

Prepared for

Brighton Company

Risk Assessment Report
Completed On: 28 Apr 2022

Powered by CONNECTWISE Identify

Thank you for taking the time to participate in this risk assessment process. The goal of this assessment is to identify your security strengths and weaknesses, and to provide advice as to the improvements you should be considering relative to your security posture.

The assessment and your results are aligned to the National Institute of Standards and Technology, Cybersecurity Framework v1.1, (NIST CSF), considered to be a best practice for firms such as yours.

The assessment spanned the five core areas of the framework as detailed below, and this report will show you results against the framework, as well as how your business aligns to other firms with respect to size, location, and industry.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• ASSET MANAGEMENT	• ACCESS CONTROL	• ANOMALIES & EVENTS	• RESPONSE PLANNING	• RECOVERY PLANNING
• BUSINESS ENVIRONMENT	• AWARENESS & TRAINING	• SECURITY CONTINUOUS MONITORING	• COMMUNICATIONS	• IMPROVEMENTS
• GOVERNANCE	• DATA SECURITY	• DETECTION PROCESSES	• ANALYSIS	• COMMUNICATIONS
• RISK ASSESSMENT	• INFO PROTECTION PROCESS & PROCEDURES		• MITIGATION	
• RISK MANAGEMENT STRATEGY	• MAINTENANCE		• IMPROVEMENTS	
• SUPPLY CHAIN RISK MANAGEMENT	• PROTECTIVE TECHNOLOGY			

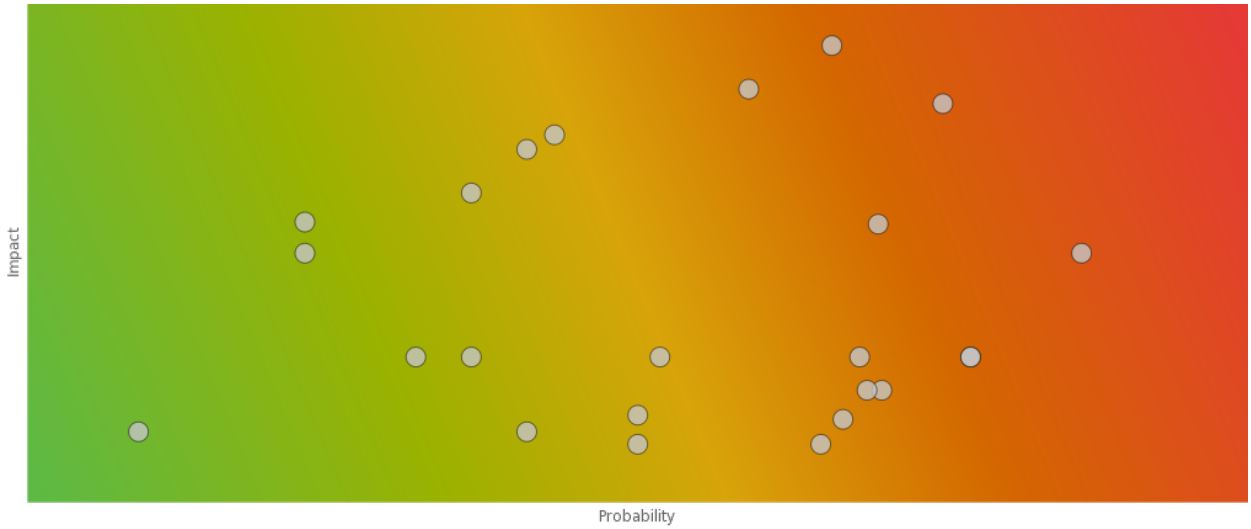
For your reference we have provided a link to the NIST Cybersecurity Framework and encourage you to download the document and become more familiar with the valuable information that can help you in your journey to better secure your business.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

OVERALL RISK ASSESSMENT

Your overall risk rating is **HIGH**

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
Critical	RS.RP-1 - Response plan is executed during or after an event
Critical	RC.RP-1 - Recovery plan is executed during or after an event
Critical	DE.AE-2 - Detected events are analyzed to understand attack targets and methods
Critical	PR.PT-4 - Communications and control networks are protected
Critical	DE.CM-1 - The network is monitored to detect potential cybersecurity events

High	ID.RA-1 - Asset vulnerabilities are identified and documented
High	DE.CM-3 - Personnel activity is monitored to detect potential cybersecurity events
High	PR.AC-1 - Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
High	PR.MA-1 - Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
High	PR.AC-3 - Remote access is managed
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. Make it a priority to 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: I don't know

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.

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

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

A: No

Importance:
It is critical for your business to be able 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: No

Importance:
It is critical for your business to be able 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.

RC.RP-1: Recovery plan is executed during or after an event — Critical

Q: Are recovery processes and procedures documented and reviewed?

A: No

Importance:
It is critical for your business to be able to respond to and recover from a security event and you don't have a process or plan to do so.

Remediation Steps:
Implement a recovery process and procedure to allow your business to recover from a security incident. Make sure to include a plan to test the process and procedure at least annually and to update it with the lessons learned from the test.

Q: Are you planning on developing recovery processes and procedures?

A: No

DE.AE-2: Detected events are analyzed to understand attack targets and methods

Critical

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

A: No

Importance:
Not being able to detect threats with an automated threat detection system is a gap in your overall security posture.

Remediation Steps:
Implement a threat detection solution that can detect threats in real time.

PR.PT-4: Communications and control networks are protected

Critical

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

A: I don't know

Importance:
A firewall is a basic technology that protects your internal network and computing assets from harmful threats coming from the internet. Not having one deployed is similar to not having locks on your doors.

Remediation Steps:
There are many inexpensive firewalls on the market today that can protect your environment. We recommend that you either research and purchase a firewall on your own or enlist the help of your MSP or IT Security Consultant to assist you in selecting and implementing a firewall for your firm. This is amongst the highest risks your company can face and should be dealt with immediately.

Q: Are you using Wi-Fi for your business?

A: Yes

Importance:
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: Other

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

A: Yes

Importance:
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: Remembered by one person

Importance:
It's risky having a person remember your Wi-Fi 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.

DE.CM-1: The network is monitored to detect potential cybersecurity events

Critical

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

A: No

Importance:
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 monitoring your IT environment for anomalous events?

A: No

Importance:
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: No

Importance:
Not performing vulnerability scans in your environment can lead to undetected threats which can be exploited within your environment.

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

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.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

High

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

A: No

Importance:
It's best practice to have a listing of all user accounts so you can make sure no accounts are left with access after employees leave.

Remediation Steps:
If you manage your own IT resources then you should create an inventory that details each user account and the devices they have access to. If you leverage an MSP for your IT resources then we suggest you work with them to accomplish this task

Q: After termination, do you disable accounts?

A: Yes

Importance:
By not disabling accounts you run the risk of an unauthorized person or persons using an account for nefarious purposes. You also lose accountability as you may not be able to prove who is actually using the account.

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: Longer than a week

Importance:
User accounts of employees who are terminated or resign should be disabled immediately, waiting longer than a week as you noted is too long. Work on a procedure to disable those accounts in a 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.

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

High

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

A: No

Importance:
The fact that you are using software applications that are not supported by the manufacturer is a critical issue that needs to be resolved immediately. Unsupported software can have security flaws which will not be patched and could lead to corruption or loss of critical data.

Remediation Steps:
Analyze your inventory of software vendors and make sure you have clear knowledge about the status of your support options.

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

A: No

Importance:
You should maintain updated licensing agreements for your software to ensure security updates and support are kept current.

Remediation Steps:
You should create an inventory of your software, determine which licenses are outdated and if your business needs require their use, then you should renew as soon as possible.

PR.AC-3: Remote access is managed

High

Q: Are user credentials shared?

A: Yes

Importance:
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:
Have an MSP or IT Consultant help you with a directory structure for ensuring that all credentials are individually owned. Doing so will force new passwords to be created for each individual and update your security policy to reflect this change.

Q: How are user credentials shared?

A: Users share other application credentials

Importance:
You should never allow users to share their password with anyone. It is used to track who had access and made changes to specific information. You are responsible for everything done on the system using your ID and password.

Remediation Steps:
It is important that all users have their own credentials and not share their applications credentials with anyone. Have someone with admin access create individual application logins for your users who are sharing credentials.

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:

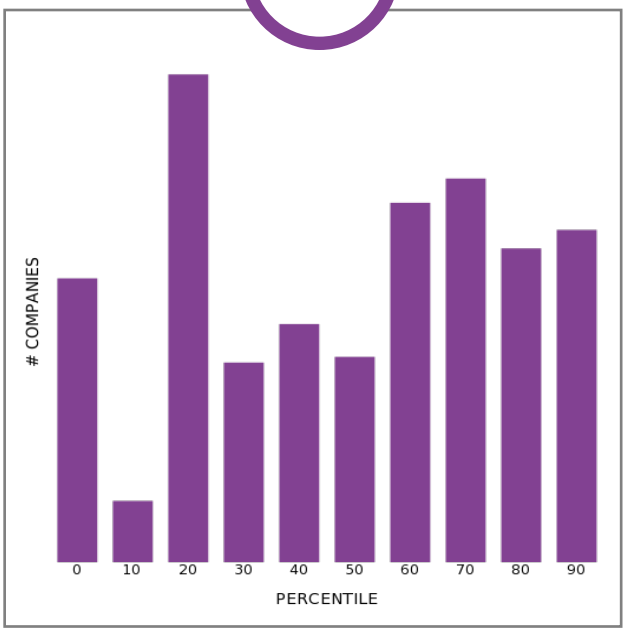
Leveraging Threat intelligence is important as you can gain vital information about your business sector that would enable you to detect and defend against known attacks. You should find out for sure if you are receiving this important information. Not having this information is a significant gap.

Remediation Steps:

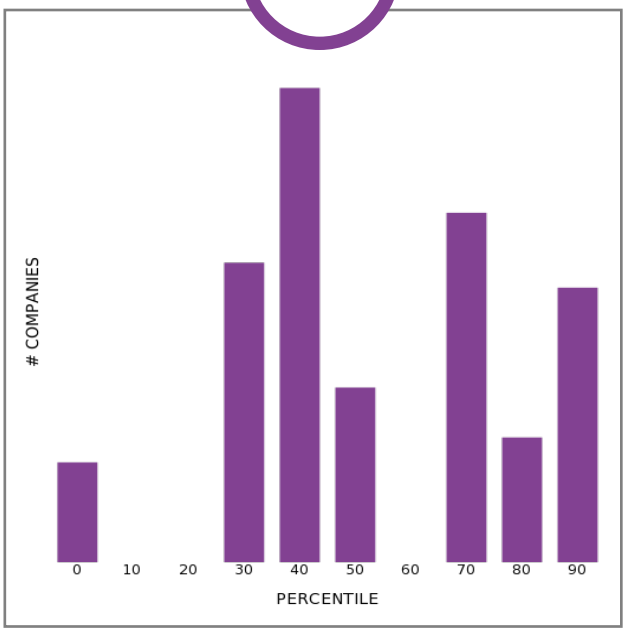
Check with your security team to see if you are receiving threat intelligence information. If you are not receiving this information seek out an ISAC that aligns to your business model and leverage the available tools on the market to enable a threat intelligence capability for your company.

INDUSTRY COMPARISONS

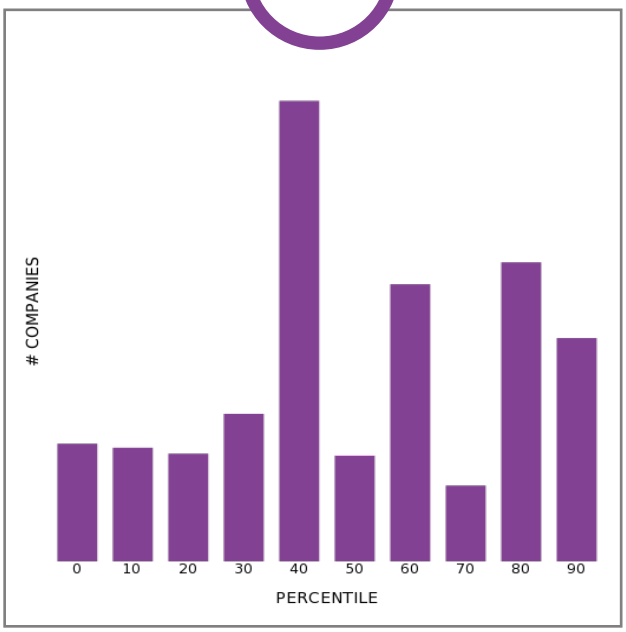
OVERALL 0TH PERCENTILE



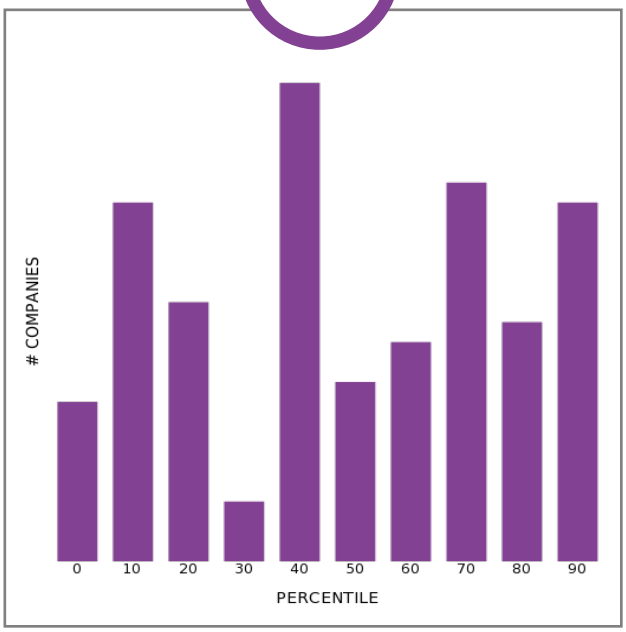
INDUSTRY 0TH PERCENTILE



COMPANY SIZE 0TH PERCENTILE



LOCATION 0TH PERCENTILE



APPENDIX / QUESTIONS

Q: Please enter your name.

> **A: Billy Brighton**

Q: Please enter your company name.

> **A: Typical Brighton Company**

Q: Please enter your role in the organization.

> **A: Managing Director**

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: International**

Q: Please enter your email address.

> **A: simon@ingeniotech.co.uk**

Q: What best describes your annual revenue?

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

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

> **A: Office staff**
> *Security incidents can happen at anytime, without continuous management you could be at risk.*

APPENDIX / QUESTIONS

> *Remediation Steps:*
> *Office staff typically do not have the skills necessary to manage your IT environment.*

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

> **A: Employees**
> *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.*
>
> **A: Friends and Family**
> *It is not good to let friends or family work on your computer systems. Your systems contain confidential data that could be compromised by others who do not have the proper security awareness training.*
>
> *Remediation Steps:*
> *Change your passwords and only allow authorized users with a need to know access the computing resources at your company.*

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

> **A: No**
> *It's best practice to have a listing of all user accounts so you can make sure no accounts are left with access after employees leave.*
>
> *Remediation Steps:*
> *If you manage your own IT resources then you should create an inventory that details each user account and the devices they have access to. If you leverage an MSP for your IT resources then we suggest you work with them to accomplish this task*

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:*

APPENDIX / QUESTIONS

> *Remove admin access or limit the use of admin access for only those occasions where it is needed.*

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

> **A: No**
> *The importance of inventories (hardware and software) is to have a record of the various components within your environment as a quick reference when vulnerabilities are identified and released to the public. This inventory should be used to identify those systems, system components, or software applications impacted by the vulnerability. Organizations can then take action to mitigate the vulnerability risk to those systems faster than if no inventory existed in the environment.*
>
> *Remediation Steps:*
> *Implement an asset management process/product.*

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?

APPENDIX / QUESTIONS

A: No
Background checks may be required depending upon the business that you are in, and even if they are not it is a good practice to understand if any past behavior of your employees may be viewed as a risk to your business.

Remediation Steps:
Create a policy that requires background checks for all new and existing employees. Notify existing employees that you will be contracting with a firm to perform these, and ensure that they are completed upon hire and annually thereafter.

Q: Are user credentials shared?

A: Yes
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:
Have an MSP or IT Consultant help you with a directory structure for ensuring that all credentials are individually owned. Doing so will force new passwords to be created for each individual and update your security policy to reflect this change.

Q: How are user credentials shared?

A: Users share other application credentials
You should never allow users to share their password with anyone. It is used to track who had access and made changes to specific information. You are responsible for everything done on the system using your ID and password.

Remediation Steps:
It is important that all users have their own credentials and not share their applications credentials with anyone. Have someone with admin access create individual application logins for your users who are sharing credentials.

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

A: No
Security policies are the guidelines that indicate management's 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.

APPENDIX / QUESTIONS

> *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: I don't know**
> *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:*

APPENDIX / QUESTIONS

> *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**
> *By not disabling accounts you run the risk of an unauthorized person or persons using an account for nefarious purposes. You also lose accountability as you may not be able to prove who is actually using the account.*
>
> *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: Longer than a week**
> *User accounts of employees who are terminated or resign should be disabled immediately, waiting longer than a week as you noted is too long. Work on a procedure to disable those accounts in a 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.*

APPENDIX / QUESTIONS

> *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: I don't know**
> *It is very important that you keep up with the latest critical updates and Microsoft Windows patches. It is very easy to probe for an unpatched computer, and once an attacker finds a flaw, they can easily exploit it with any number of scripted attacks. Having a sound patch management process is the most effective, and the easiest way to defend against such threats. Operating system and software application vendors regularly release patches for their products.*
>
> *Remediation Steps:*
> *Update or create a patch management process and policy. Most operating system and application vendors release patches regularly, and you should ensure that you apply and validate that the most critical patches are applied, at the very minimum.*

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

> **A: No**
> *The fact that you are using software applications that are not supported by the manufacturer is a critical issue that needs to be resolved immediately. Unsupported software can have security flaws which will not be patched and could lead to corruption or loss of critical data.*
>
> *Remediation Steps:*
> *Analyze your inventory of software vendors and make sure you have clear knowledge about the status of your support options.*

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

> **A: No**
> *You should maintain updated licensing agreements for your software to ensure security updates and support are kept current.*

APPENDIX / QUESTIONS

> *Remediation Steps:*
> *You should create an inventory of your software, determine which licenses are outdated and if your business needs require their use, then you should renew as soon as possible.*

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

> **A: I don't know**
> *A firewall is a basic technology that protects your internal network and computing assets from harmful threats coming from the internet. Not having one deployed is similar to not having locks on your doors.*
>
> *Remediation Steps:*
> *There are many inexpensive firewalls on the market today that can protect your environment. We recommend that you either research and purchase a firewall on your own or enlist the help of your MSP or IT Security Consultant to assist you in selecting and implementing a firewall for your firm. This is amongst the highest risks your company can face and should be dealt with immediately.*

Q: Are you using Wi-Fi 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: Other**

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 Wi-Fi 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: Old equipment is not disposed and kept in storage
It's important to dispose of old equipment and the data that resides on that equipment. But you need to check that you are removing all data before doing so.

Remediation Steps:
Implement a practice to remove data from old equipment before disposing of the equipment. The drives should be wiped of data using at least 3 passes of deletion. Reference these DoD standards for media sanitation https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

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. Make it a priority to sign your employees up for annual security awareness training.

APPENDIX / QUESTIONS

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

> **A: No**
> *Not being able to detect threats with an automated threat detection system is a gap in your overall security posture.*
>
> *Remediation Steps:*
> *Implement a threat detection solution that can detect threats in real time.*

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: No**
> *Not performing vulnerability scans in your environment can lead to undetected threats which can be exploited within your environment.*
>
> *Remediation Steps:*
> *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 for your business to be able 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.*

APPENDIX / QUESTIONS

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

> **A: No**
> *It is critical for your business to be able 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: Which of these activities do you perform to improve organizational response activities? (Choose all that apply)

> **A: Other activities are performed**

Q: Are recovery processes and procedures documented and reviewed?

> **A: No**
> *It is critical for your business to be able to respond to and recover from a security event and you don't have a process or plan to do so.*
>
> *Remediation Steps:*
> *Implement a recovery process and procedure to allow your business to recover from a security incident. Make sure to include a plan to test the process and procedure at least annually and to update it with the lessons learned from the test.*

Q: Are you planning on developing recovery processes and procedures?

> **A: No**