Audit Plan for Tax Service

Purpose

The purpose of this audit is to review software security along with physical security and evaluate risks in the small organization's everyday systems.

Outcome

The outcome of this audit will be recommendations for the owner of the tax service.

Scope

The scope of the audit is the Internet connection, computer, and data processes.

Audit Procedure

Arrival: The auditor/audit team will arrive at the home office and contact the owner for an access code/access/authorization to proceed. Auditor/audit team will then walk into the facility using the code/access/authorization to gauge staff reactions.

Introduction: Once auditor/audit team is satisfied with the entry exercise they will introduce themselves to the owner.

Audit Meeting: Once introduced, the auditor/audit team will work with the owner and any members of the staff, as requested, to complete the attached audit plan documentation. Items may be added to the audit plan as necessary and as agreed between the auditor/audit team and the owner. These items will be documented using the blank lines in the audit plan.

Audit Hot Wash: Once the auditor/audit team has completed the attached Audit Plan document the auditor/audit team will inform the owner that the audit is complete and will then conduct a post audit meeting with the owner. The purpose of this meeting will be for the auditor/audit team to convey initial findings and for the auditor/audit team and the owner to generate and agree on any needed action plan/further information needed/potential recommendations/etc..

Audit Commenced (time/date): 4/23/23 8:00AM **Audit Complete (time/date): 4/23/23 11:00AM**

Auditor: Samantha Leahy

	Audit Plan: Items and Observations Auditor: Samantha Leahy			Date: 4/23/23
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/No)**
1	Check entry security	Access code in place or locked home/office door since this is located at a home office	Password on front door to enter the home where home office is located, no lock on home office door	No
2	Check location of router	Location of router in secure location, no hazards	Location of router in living room, no password on router, no hazards around router	Yes
3	Check location of computer used for organization	Location of computer in secured spot, access only for business need	Computer is in a secure home office, family members in household aware of business, no lock on door if guests are here	No
4	Check password strength of computer	No exposed passwords using HaveIBeenPawned, no passwords written down or saved on computer	Using HaveIBeenPawned, password has been exposed at least 1 other time, no passwords written down	No
5	Check current computer security system against attacks	Current system has security software in place to protect against malware and/or other attacks	Has been recommended by IT specialists that Windows security will suffice for current system	Yes
6	Check if systems are up to date	Current system is up to date	Systems are up to date on computer, software used there is an update that needs to be done	No
7	Check ports using Shields Up	Ports are in stealth or closed	All service ports and common ports are in stealth or closed	Yes
8	Review computer files for personal use vs work use	Ensure files are protected and access for only business use	Personal files and professional files are kept in separate places on the system. Only owner has access to system	Yes

9	Review plans for possible outages on power or internet connectivity	Plan in place that keeps the work flowing if outage were to happen with power or internet connectivity	No plan in place – no regular work hours, but if something due that same day unable to complete	No
10	Check for knowledge of possible phishing attacks using links for phishing quizzes	Knowledge of phishing attacks, able to identify what a phishing attack looks like	Passed phishing quiz used during class, has knowledge of possible phishing attacks	Yes
11	Check for secured router password	Router password secured and not open to the public	Password is not exposed on router	Yes
12	Check if asset inventory exists for small organization	All organization devices are accounted for	No asset inventory	No
13	Ensure access controlled on business systems	Business systems only used for business need and only by people who are authorized	Only owner accesses computer with client information, password in place for computer	Yes
14	Check if personal devices are used for professional purposes	Personal devices separate from professional use devices unless plan in place	Personal devices are used for professional purpose, but only access by the owner	Yes
15	Check if any contingency plans are in place	Contingency plans in place	Identity protection in place if client information was to be exposed	Yes
16	Check if devices are accessed by anyone other than owner	Business devices accessed by only the owner (only employee in business)	Personal devices used for businesses purposes, but only used by owner	Yes
17	Check physical storage of documents	Secured physical storage of documents, organized and locked	Keeps in envelopes, and stacks on desk	No
18	Check that client information is secure	Client information secured	Computer has a password, clients files do not	No
19	Check that client information in system is organized	Client information organized	Each client has a file along with an ID	Yes
20	Ensure correct disposal of unneeded documents	Correct disposal of unneeded documents	Dispose of unneeded documents immediately with a shredder	Yes

What we did –

I found a small organization, a tax service that is owned by a family member, and completed an audit on the security systems that are in place as well as the physical security. We went through and discussed topics such as password protection, security measures with software and physical assets, possible plans that can be put in place if none existed, and the risks of not having a security system in place to protect the business systems from being compromised. I was able to list certain aspects of the business system that needed to be checked, but I also took recommendations from the owner and asked them if there were other things besides what I listed that they wanted to investigate. I explained to the owner that we would determine whether each description being checked would pass or fail and at the end of the audit, I would recommend measures to put in place that I have learned from class. There were websites that I used from class such as HaveIBeenPawned, to check password strength/exposure, and ShieldsUp to check if the ports were closed or in stealth condition.

What are the results –

For most of the checks, the owner did pass, but there were some that did not pass. Since the organization was in the home office, I checked the entry security to the home and found that there was a passcode on the front door, but no lock on the home office. The door could be locked from inside of the room, but not from the outside. If guests were to visit, they would have easy access to this home office which did indicate possible risk exposure to confidential files and/or client information. Another fail that fell under the same category was the business computer location. This computer is in the home office and guests being able to access the office also applies in this scenario.

Another top finding that was not passed during the audit was a secure password. I was able to share the website used during class of HaveIBeenPawned to check if the password that the owner used was secure and had not been exposed. The results on the website showed that the password has been exposed at least one time.

Another check that was conducted was to make sure that the software systems were up to date. The owner uses one computer for the tax service business and had one major software that is used. The computer system was up to date, but the tax software was not up to date. The owner did explain that this update was added recently but did not take advantage or automatic updates or having the update done more efficiently.

I asked the owner of the business if there were plans in place if the power were to go out or internet connectivity since the business is home based. There were not any plans in place if either of those were to go out. The owner explained that there were not regular said hours for the business, but that if they needed to get something done that same day and the power were to go out, they did not have a plan in place to keep the workflow.

I explained that we had learned how to conduct an asset inventory in class and asked if the tax service business had an asset inventory. An asset inventory did not exist for the business. Another top finding that was of severity was the security of the client information whether that be on the desktop or physical. The owner does keep the professional information in separate files on the computer since this is also used as a personal computer. The computer itself does have a password and is only accessed by the owner, but there is not an access code on this information in case anyone else were to have access to the computer. Regarding physical information, the owner did have information on their desk that could be put away and locked in a filing cabinet.

Recommendations –

Entry security and location of business computer – Since there were security measures to enter the home, I recommended an additional security measure on the door of the home office. The door is currently able to be locked from the inside when working, but I suggested a new doorknob that would also allow the door to be locked from the outside when not in use. This would be of little impact to the

business compared to finding a new office to add more security measures. I recommended this be completed within a week.

Secure password – I recommend changing passwords every three months. The owner does not currently write down passwords, but I did give a reminder to keep passwords secure, writing them down was not good practice. I also recommended setting a reminder to have these passwords changed. This recommendation has little impact on the business. It will take little time to set a reminder to change the password and does not cost anything to ensure regular password changes.

Staying up to date with software – To have very little to no impact on the business, I recommend having automatic updates set up if that was an option. If that was not an option, I did recommend having the updates completed as soon as possible to keep the system safe from being compromised. There was a current update to complete, and I recommended having that completed within 24 hours.

Asset inventory – Although this was a small business with one employee, I do recommend having an asset inventory. Based on my experience from class, I explained how helpful it was to have an inventory which could also include plans, measures, and preventions in place to have little impact on the business when it comes time. I recommend having this completed within 2 weeks.

Security of documents physically and electronically – For electronic documents, since the business has one folder with client information, I recommended setting a password on these files for only the owner to access. This is at no cost to the business and would add an extra security measure when it comes to confidential client information. I recommend a timeline for this to be done within 3 days. Regarding physical documents, I recommend having a filing cabinet and a lock on the filing cabinet. The business does well about shredding needed documents, but have a secure system for the physical documents would add more security and less exposure to confidential information. I recommend having this completed within 3 days as well. This will have little impact on the business since money will be spent and time will be needed to find a filing cabinet and have a filing system.

Risk posture –

Based on the audit plan completed for the small tax service, the greatest risks are possible exposure to client information and password strength. The greatest vulnerability for the business is the possibility of being compromised due to not keeping software up to date. The home office is also vulnerable due to not being secure if guests were to come to the home and enter the office. I did explain these risks to the business and made recommendations that would be beneficial and smooth for the business.