**What We Did**

To begin this security audit, the first step was to initialize a purpose, outcome, scope, and procedure outline to gain cognizance of the business and what needed to be observed. During this stage, items numbers and expected findings (pass criteria) was formatted in preparation for the audit meeting. Once this section of the document was finalized, important contacts of One Stop Remodeling were notified of the audit being completed and a time was scheduled for the audit to take place. The owner reached out and asked if Friday would work, to which a time of 2:00 PM was decided on. We agreed I would meet him at the premises and his foreman, Tanner Jones, would be present as well.

Upon arrival on Friday, I contacted Tanner Jones for access and asked him to give approval for the audit being done. He agreed and led me into the premises through the front door. Within the first few minutes of being present, I noticed it was a quiet atmosphere and the only people there were Tanner and the owner, Joseph. I looked around and didn’t initially notice any serious threats on the surface. It appeared to be a smaller scale operation without much background noise. There was only one office used for conducting business and it was located towards the back of the building. After I conducted my entry exercise, I met with Joseph Skinner and began the official audit.

The total time for the audit took approximately one hour and forty-seven minutes to report my findings on twenty observations. The owner, Joseph, and this staff member, Tanner, were both notified when I was finished with the audit plan to which we then sat down and went over the results. Here, we discussed action plans and recommendations that would fit best for the company and company budget.

**What are the Results?**

1. *Windows are locked when room unattended.* This expected finding was unfortunately not observed, a single window in the bathroom of the building was left unlocked. This could introduce a huge problem with breaking and entering/ theft.
2. *Staff trained on cybersecurity manners.* When performing the audit, customer communication was found to be taking place mainly through Facebook Messenger. This was happening on staff cell phones and on the owner’s cell phone/ laptop computer. Even though Facebook Messenger is equipped with a default end-to-end encryption, there was no additional security to get through once you obtained the cell phone. This could put sensitive customer data at risk as finances and addresses were being sent through this channel.
3. *Stable internet connection.* Upon inspecting the businesses internet connection, I noticed the router itself was in a secure location with the appropriate security setting configured. However, I took liberty to test the internet speed, and the results were less than desirable. Download speed checked in at 36.41 Mbps and upload speed at 37.06 Mbps. I used a site on the internet to conduct this examination and ultimately it showed the connection was not suitable for a company to conduct daily operations. The owner did state he had been experiencing issues but was under budget restrictions.
4. *Digital signatures require authentication.* The owner consistently uses Adobe Acrobat for contract purposes to which often require a signature. He does have an e-signature set up with this program and it is accessible without authentication. This poses an array of threats as if the computer were ever left unlocked or even hacked, his signature could be used for several malicious reasons.
5. *Business has a clear plan for incident response.* My findings showed there is no existence of an incident response plan nor is there any history of one. This is an issue as he has several other employees that work for him and if one were to get hurt on the job, it could pose major liability problems.

**What are Your Recommendations?**

1. *Windows are locked when room unattended.* My recommendation for this obstacle is to ensure all windows are locked and secured. An additional measure the owner could take would be to purchase a window security alarm for the room that contains sensitive documents and devices. They can be purchased on any online retail site for as low as $10 for a set of two. This is a budget conscious way to induce heightened security and allow for response time if there ever was an imminent threat. I would recommend this takes place on an instant timeline as I had the owner lock the window before I left.
2. *Staff trained on cybersecurity manners.* To address this issue, I would recommend all staff (and owner) that participates in the communication with customers to add an app lock to Messenger specifically. To do this, you would hold down on the Messenger app and select “Require Face ID” or “Require Passcode”. This simply adds another layer of security to private data. It is also a free method, and I would also recommend an instant timeline as I showed them how to do it before I left. For other staff members that were not present at the time, I would recommend this to be done within the following week.
3. *Stable internet connection.* As the internet was not up to par with what would be ideal for business operations, I would suggest the owner shop around for better internet that could fit his needs better. As this could be a pricier option, I will assign a timeline of 45 days to gather the necessary budget requirements and allow time to find a match.
4. *Digital signatures require authentication.* As this was a failure on the audit, I recommended the owner start using DocuSign; DocuSign is a perfect site for handling contracts while also keeping documents and signatures under two-factor authentication and password. I assigned a timeline of 45 as well, as I understand it could take time to switch over to a new program as well as gather the budget to do so. The plan that would work best for this business is $25/month and includes unlimited contracts.
5. *Business has a clear plan for incident response.* I recommend an incident response to be implemented and even to include other events such as cyber-attacks. I suggest it be reviewed by each employee and regularly updated. I assign a 30-day timeline for this as it is an overdue process.

**What is Their Risk Posture?**

Based on the overall observations of the security audit, the risk posture of One Stop Remodeling presents multiple vulnerabilities that require immediate attention. This business currently faces a moderate to high level of risk in various areas as mentioned above. I would recognize the greatest risk to be unsecured communication channels, which are those taking place through Facebook Messenger. Although the app offers end-to-end encryption, it does not protect the device itself from unauthorized access. Their greatest vulnerability could be found in the lack of authentication on digital signatures. Without authentication, an unauthorized person could easily misuse the owner’s signature. In conclusion, the overall cybersecurity threat One Stop Remodeling faces is the absence of an incident response plan which would include what to do in the event of a cyberattack or data breach. Without this, action would be delayed and further damages could be caused.