Megan Moore
Buff ID: 1014735

Completed Security Audit - Lucifer Lighting

The purpose of the security audit was to check the configuration and security of the computer server and router at a lighting manufacturing company, Lucifer Lighting. This was a previous employer so they are willing to work with me for this assignment. I stay in contact with many of the employees. As the firm's main focus is design engineering, cybersecurity and protection of their CAD based designs is of upmost importance. While reviewing the security of the computer systems, the physical security and security processes of the manufacturing buildings was also reviewed for comments.

I was the main auditor and I arrived at the facility Monday morning on November 14th. Once I arrived, the front desk contacted the IT manager, Hector Green, for authorization to proceed. Permission had already been previously requested to the CEO and facility manager. This was obtained viz a conference call had previously to explain the audit request and what the procedure detailed, along with how the results would be shared back to management. Since permission was granted by leadership and there were no manufacturing or network issues this morning, we were able to conduct the security audit.

After a brief walkthrough of the facility with Hector, the group was joined by the facility manager, Dave Nosal, to complete this exercise. We continued the walkthrough to the security area. Once there, the auditor team worked with the IT department members and any members of the staff, as requested by the facility manager, to complete the attached audit plan documentation and make notes for any additions. Any additions were documented using the blank lines in the audit plan or separately by the IT manager. The auditor team agreed that the scope of the audit is the computer engineering server and data processes for storage and backup. The team also agreed that the outcome of this audit would be recommendations for the owner of the manufacturing firm and IT manager.

During the course of the audit, there were a number of discoveries. The top five findings have been included in this document, with the remainder comments all being saved by the IT manager and facility manager to later address with management.

1. Network password: Severity – Medium.
   Recommendation and proposed Timeline: While it was determined that the company was performing best practices of routinely changing the password for its network, where it lacked was in the storage of these passwords. Currently, all passwords are kept written down for records in one notebook. This notebook is typically left out in the IT department for access as needed. Immediate proposed change was to move this notebook to a more secure location, such as a locked file cabinet or locked drawer of the IT manager, so as to prevent theft. Should anyone in the company, with network access or not, gain access to this office then they would be able to also gain access to multiple passwords.

2. Lack of cloud back up system: Severity – Medium.
   Recommendation and proposed Timeline: Like many individuals, the CEO is weary of trusting online cloud systems for proprietary information especially for information that is of critical value to the company and brand. Cloud systems have security breaches and due to this, the CEO has always been reluctant to use anything other than physical backups. Currently, hardware based backup systems are in place but these have risks noted in finding 3 and 4. The IT manager has also mentioned this gap to the CEO before but will require more extensive research to

determine a dependable cloud system to use. Timeline for research is end of year so the CEO can make a decision for 2023.

3. Climate control of server location: Severity – High.
   Recommendation and proposed Timeline: This finding is more complex to address and more costly due to the financial cost of adding additional ventilation and controls to the server location. The severity of this risk is noted as high due to the CEO's reluctance to rely on cloud based security backups and only using hardware based backup systems. These physical on-site backups need good air flow and climate control to function properly. The CEO will be reviewing the specifications of the servers to determine the updates needed but due to supply chain and inflation, will address this item before the next summer weather period here in Texas.

4. Lack of surge protection: Severity – High.
   Recommendation and proposed Timeline: This finding is the simplest to address with the smallest financial impact to the company. The IT manager will be addressing this by adding a surge protection device immediately (by next day). This will not disrupt business operations at all but be the first step in building a more secure network and risk posture for the company.

5. Lack of deactivation of old user profiles: Severity – Medium.
   Recommendation and proposed Timeline: While a user would need to be on-site in order to utilize the network, leaving old user profiles active is a large risk for cybersecurity. Someone with ill intent could access the network due to other findings in this audit and do irreparable damage. The audit team agreed this could be immediately addressed with the removal of the old accounts in order to build a more secure risk posture for the company.

The above findings and this document with the completed Audit plan will be presented to the CEO. Further detailed comments found too informative for this document will be saved by the IT manager and facility manager for the CEO's records. We were unable to hold a post audit meeting with the CEO due to availability, however an email was sent along with hard copies delivered to their office. The results describe any needed action plan which should be put in place to resolve any alarming findings, detailed here or in the additional document the IT manager has on-site. With the audit concluded, the risk posture of the company can be defined and improved upon.

Risk posture is defined by the overall state of an organization or individual's security and defense against cybersecurity attacks. How well it is able to manage and strategize the prediction, prevention and response to threats and vulnerabilities to software, hardware, networks, services, and information. Maintaining a constantly updated status is gravely imperative to ensure the enablement of an agile, adaptive and evolving security infrastructure.

As part of the exercises this semester and in this Security Audit, a robust risk posture is built by identifying assets, the risks to those assets, documenting security controls, being realistic and thoughtful as to who or what can be targeted and establish responsibility with a plan. This security audit was very insightful for two reasons: the company will benefit from my observations and I also gained personal understanding of how to improve my own systems at home and my behaviors in public.

Megan Moore
Buff ID: 1014735

After conducting the audit, I sat down with Hector and Dave to review our findings. The greatest risk to the company's cybersecurity at the present is their lack of deactivating old employee accounts. Anyone, whether a previous employee or impersonating one, could obtain access using one of these nonactive accounts as long as they were in range of the network. This could create a very real threat to the company's intellectual property of designs, which is of extreme importance and value. Theft of these items would cause severe brand damage. Secondly, we determined the greatest vulnerability the existing security system has is the lack of a cloud-based backup. While steps had been taken to ensure a hardware-based backup was in place, these can fall through due to subsequent findings of the lack of surge protection and poor climate control of where the server is located.

Overall, completing both the Audit Plan and Final Security Audit using the plan was very enlightening as to what additional things I should be aware of regarding cybersecurity risks. I've since learned that any enterprise or individual's cybersecurity posture should take the following into account:

- Security status of assets, both software and hardware, networks, services and information
- Controls that exist and are in place to protect from attacks
- Ability to measure and manage your defenses
- Ability to react and recover if an attack occurs

Without addressing all of the above, the company or person is left vulnerable to the fallout of an attack.

Megan Moore
Buff ID: 1014735

	Completed Audit Plan: Lucifer Lighting **Items and Observations** **Auditor: Megan Moore, Hector Green, Dave Nosal** **Date: 11-14-2022**			
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/No)**
1	Check network password strength	Should be strong: no dictionary word	Password protected but password is not routinely updated. Also password log kept written down in office.	Yes, but suggested improved frequency of password updates. Also the written log should be locked away in a secure location.
2	Check ports using shield's up	Ports are in stealth or at least closed	Yes, ports are stealth or closed.	Yes
3	Check for missing updates; versions of software	Computer is up to date with auto updates on	Updates are done regularly on the weekends but sometimes do not finish installing without someone present meaning either an IT employee must be there over the weekend or the system updates are delayed until Monday.	Yes
4	Cloud backup system in place	Back up exists; functioning correctly	Hardware backup exists but no cloud based system. If hardware fails, this could be a major setback.	No. Recommended to establish cloud system backup.
5	Server is kept in a location with controlled access	Access is limited to those with a need	Door is kept locked with only a few keys with known individuals who have been granted access.	yes
6	Review computer system files for possible malware	No malware found; antivirus software in place	Antivirus installed. Updates however are not turned on and must be done manually. While this might minimize downtime for the manufacturing lines, this could be improved.	Yes
7	Check for access control settings for server	Only IT manager or department can access all files	Only IT manager and department is capable of accessing all network server files.	Yes
8	Check for surge protection on power supply	Surge protection present	No surge protection.	No

Megan Moore
Buff ID: 1014735

9	Check server and router in location with temp control and good air flow	Air flow and temperature in acceptable range	Temp control in place but needs improvement and more air flow. Risk to hardware if ventilation fails in hot weather.	Yes
10	Ensure router is password protected	Password is active	Password is active	Yes
11	Ensure access controlled on all business systems with user profiles	Access is controlled; all users assigned profiles	Access profiles not always deactivated when employees leave	No – access profiles controlled when setup but not deleted. If not careful, someone could breach the system using an old login.
12	Ask about a security plan	Security policies are in place	Basic property security in place but nothing specific to server or network	No
13	Building security	Is there protocol in place for theft; insurance policy coverage	Insurance policy exists; property has security presence in evenings and weekends	Yes