Risk Assessment Table

| (1) Asset or Operation at Risk | (2) Hazard | (3) Scenario (Location, Timing, Magnitude) | (4) Opportunities for Prevention or Mitigation | (5) Probability (L, M | Impacts with Existing Mitigation (L, M, H) | | | | | (11) Overall Hazard Rating |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | (6) People | (7) Property | (8) Operations | (9) Environment | (10) Entity | |
| Social media page | Ads | Malicious actor could copy ads with links that contain malware<br>-Malicious actor cause impeccable damage to company's name | -input a cyber attack learning curriculum to combat against such attacks to bring awareness to customers and employees alike | H | H | H | H | H | H | MH |
| Web Application | User Authentication | -Malicious actor penetrating through the week authentication protocols | -implement more robust authentication protocols withing the SQL | M | H | M | H | H | H | MH |
| Server | Access Control | -Malicious actor getting into the server room via social engineering skills | -Awareness training for all employees to prevent unauthorized access to areas | H | H | H | H | H | H | HH |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Web application/database | SQL Injection | -Malicious Actor implementing an SQLi attack | 1. Use of prepared Statements (with parameterized queries)<br>2. Allow-list input validation<br>3. properly constructed stored procedures | M | H | L | H | M | H | MH |
| Database | Access Control | -Employee who completes orders has access to HR department data<br>-Root is not password protected | -Restrict access to the SQL Server Database.<br>-Make sure the root account in the server is password protected | H | H | L | H | H | H | HH |

The overall risk assessment details categories as to why there may or may not be an increase in the overall security risk. This is not to say that there could not be other ways alleged attackers could get access to your network. Another thing to keep in mind is that when completing this risk assessment, one must be aware that considering circumstances or updates there may be an unforeseen risk associated with certain circumstances and updates that the company may have to go through. Let us dive into the overall analysis laid out in the risk assessment table.

Starting off with the social media page and its overall risks. This is more than likely how the business is going to reach the local population and promote its business. That means that there is a risk in having a media marketing scheme. When it comes to any media marketing there is the risk of the employees becoming vulnerable to social engineering attacks such as phishing attacks that are almost exact copies of the company's ads, a customer clicks on this ad and is immediately taken over by malware, then that customer bad mouths the company for terrible ad practices. The thing here is that the company is not to blame per se, but the customer's ignorance caused them to be acceptable to the attack. Implementing an active awareness to customers could in turn keep the company from becoming a victim of malicious attackers.

User Authentication is one of the bigger risks in the world of web applications and can be the different overall successful business application or it being tanked. The business needs to consider that there are many users that will have access to the database. This can be anyone from an employee to a customer placing an order online. If users have access to areas of the database that they should not this can pose huge risks to the company as a whole and in turn, be the precursor to a breach that would cause the company to face bad mouth accusations and could result in serious revenue losses. To prevent and mitigate such a risk there needs to be an extensive protocol implementation with employees and how the user authentication needs to be set up in the database (SQL Injection Prevention - OWASP Cheat Sheet Series, n.d.).

One thing we must keep in mind when completing the risk assessment table there are a lot of risks involved within any business and nowadays there are more data vulnerabilities than there were 5 to 10 years ago. The physical applications of servers and databases cannot be ruled out. When it comes to servers and databases knowing who has access is just as powerful as knowing who the owners are. That means that whoever has access needs to have a clear understanding of protocols entailing what happens after an id is lost, along with the repercussions of losing said id. One such thing the company can do is make sure that these servers are protected by some type of biometric authentication. Another thing the company could do is make sure that the employees are educated on social engineering attacks that malicious actors use to gain their trust and gain access to things such as server rooms and other parts of the company (Ellingwood & Garnett, 2022).

## References


1. *SQL Injection Prevention - OWASP Cheat Sheet Series*. (n.d.). Retrieved October 31, 2022, from https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
2. Ellingwood, J., & Garnett, A. (2022, May 19). *Recommended Security Measures to Protect Your Servers*. DigitalOcean Community. https://www.digitalocean.com/community/tutorials/recommended-security-measures-to-protect-your-servers

Home Improvement

**Department / Function / Process Operational & Financial Impacts**

| Timing / Duration | Operation Impacts | Financial Impact |
|---|---|---|
| Social Media Page –<br>• March-late June / > 1 month | Drop in site visits to lack of advertisements, Loss of customer influence, Delay executing a business plan or strategic initiative | This could total to a 20,000-dollar profit margin lost to discounts missed or a missed link not clicked due to the site being down |
| Web Application<br>May-Aug / 15min | A very significant drop in sales/loss of web application data | This type of attack lasting this long could potentially result in customer integrity loss and could result in a 160,000-dollar loss if not more long-term |
| Server<br>May-Aug / 15min | Loss of data/loss of customers / Loss of Revenue | This type of impact would be bad as having your in-store transactions linked together along with web transactions and the servers go down the company has the potential to lose at least ¼ million due to long-term effects and short term |
| Web Application / Database<br>Anytime / 15min | Loss of online and in-store inventory data/loss of revenue / disgruntled employees | This would not stop all services but would cause issues with online web functionality / It would also create frustration with customers and would result in a loss of almost ¼ million dollars in lost revenue as well |
| | | |

1. Social Media: There is a lot that goes into social media whether it be an advertisement or just building a good customer base via social media. This needs to be considered in the risks to the company, especially when it comes to the over-profit margin and risk that can be associated with social media. With if the social media site were to get hacked the company would lose a significant amount of profit margin to the deals missed, because the advertisements for specials may have been only seen on the social media page because they do not go to the store directly. The social media page being down will also lead to disgruntled employees that depended on the posts to get deals they would not have seen otherwise. Another aspect to keep in mind as the ads and promotions being placed here that were put into the business model to promote the business would also deplete as well if the social media site were to go down. Along with losing a profit loss of 20,000 dollars due to lost promotions
2. Web Application: Here we have the web application associated with the business. This plays a big part in the business's revenue and associated promotions. If the web application were to go down due to a cross-scripting attack that could lead to the site being down and the company losing revenue of 160,000 dollars (Cross-Site Scripting (XSS) | OWASP Foundation, n.d.). This will also lead to the company being in complete shambles with the web page being down the customers will not be able to look up deals on their own and there will be an influx of customers needing more questions answered which could lead to a bottleneck at the customer service counter. This in turn will lead to possible security gaps in the customer service counter, which could lead to stolen even more stolen assets.



3. Server: The server for the company is what links the company to the banks and the database storing inventory data and customer data. If the server goes down, there is room for a big loss of profit and potential customers. This is because it will be hard to link with banks to run transactions in the store and these days hardly anyone carries cash so there will be a loss of revenue during the time the

servers are down. This will also lead to potential inventory losses if anything is sold while the servers are down, the inventory cannot be updated and there are no checks and balances for what was sold and returned. This can be avoided by making sure that there is a contingency plan to either stop sales if the servers go down or to have some way to keep track of the data and input it once the servers are back up so you do not lose potential business but also can keep the business running. Either way, the company would have a significant loss of about ¼ million including the lasting backlash from servers going down and there not being a plan.

4. Web Application / Database: In a situation where the web application and database went down there would be a big drop in online sales along with lost data. The issue with the lost data is that customers who may have made an order may end up losing the order completely and that could lead to bad reviews for the web application. Another aspect to keep in mind is that there could be the potential for customers' data to be stolen which would lead to a big trust gap and the customer may never shop with the company again. There are a lot of things to keep in mind and the biggest issue is the potential losses if issues that could cause these problems were to be left unchecked.

References

1. *Cross-Siteite Scripting (XSS) | OWASP Foundation*. (n.d.). https://owasp.org/www-community/attacks/xss/

1. Disaster response plan

    a) Introduction

        i) The Main purpose of this plan is to make sure that we cover the basis for the business to keep running in face of disaster and/or damage

        ii) In this plan we will cover Risk assessment, Business Impact Analysis, and Resumption strategies. This is to ensure the understanding of the plan and to make sure there are no gaps within the plan

    b) Risk Assessment

        i) We have identified several risks within the company including access control, user authentication, and SQL injection.

        ii) There are risks and there are mitigation strategies for these risks. For the access control portion, there need to be guidelines for each part of the company as to who has access to what (fe HR has access to pay and employees have access to taking payments and inventory and there is no access granted to all users). With user authentication, there needs to be some form of password protocol to make sure the password cannot be easily hacked into. This also goes into setting up some form of double authentication via password and phone/password and email authentication, to make sure the person logging in is in fact who is logging in and not a malicious actor. Then the company has also an issue that affects a lot of web applications and that is SQLi injection. This can be prevented by making sure that prepared statements are used along with allow-list input validation.

    c) Business Impact Analysis

i) With the implications of malicious actors and human error the company needs to be ready at any given notice. This means that there will be impacts on the company and overall, the impact is high if the risks are not adjusted for. The overall costs will be in the range of about .5 million dollars if not addressed and taken care of. The reasons are the downtime of the database due to SQLi, as well as losing portions of data due to the lack of access control protocols being implemented (*Business Continuity Plan | Ready.gov*, n.d.).

ii) In the impact analysis worksheet, you can see the overall analysis of the issues that are going to be faced if the company is not prepared. Looking at the table the

TIME/DURATION is what goes down and a projected amount of time it could go down for.

Operation Impact would be what would be impacted by this process being down

Financial Impact Is the projected losses that the company would lose just from this process being down for the certain time (*Business Continuity Plan | Ready.gov*, n.d.).

d) Resumption Strategies

i) There are a lot of options available to the company that can allow it to get back up in running when faced with disaster or damage to web application services. This can include a double server that could allow for one server to pick up slack if the other server were to go down so customers can still order and do what they need to do until the other server could be fixed. Another option is to have a completely isolated backup server until you there is a problem, and it has to be switched manually to get the site back up and running

ii) When It comes to making sure your company stays running the most preferred is a warm site. With a site such as this it is not fully running like a HOT site would be but it has all the hardware and servers you need to handle the load but the data would need to transferred from the active site upon the disaster to bring this site current. It is also faster to get up and running than say a cold site that doesn't have the computers and such to make a quick switch like a warm site would and takes twice the time to get up and running.

2) IT incident response plan

a) Introduction

i) The sole purpose of this plan is to provide procedures and tools to help eliminate, identify, and recover from cybersecurity threats.

ii) In this plan what will be covered is preparation, Identification, containment, Eradication, Recovery, and lessons learned from all cyber events.

b) Preparation

i) In this part of the IT response plan the main goal is to perform a risk assessment to identify the most sensitive assets.

ii) This will include a communication plan, document roles, and responsibilities, and recruiting members to the cyber incident response team (CIRT).

c) Identification



i) With this part of the Incident Response plan the IT team should be able to detect any deviation from normal functionality and traffic.

ii) Determine the severity of the incident and document the "Who, What, Where, Why, and How".

d) Containment

i) Short-term Containment

(1) This type of containment will consist of isolating the network segments with the infected hardware and taking down production servers.

ii) Long-term Containment

(1) This section of the containment portion is where temporary fixes will be done on the affected systems to keep production going while rebuilding clean systems (Cassetto, 2022).

e) Eradication

i) The IT team must identify the root cause of the attack and remove any malware or viruses that may be present.

ii) With this if any vulnerability were to be exploited then it should be patched immediately.

f) Recovery

i) Here it is paramount to make sure that the IT team brings the production systems back online carefully, to ensure another incident does not occur.

g) Lessons Learned

i) When the Team has effectively completed the above complete documentation of the incident should be done no later than two weeks from the end of the incident.



ii) The team will take the information gathered here and use it to critique their overall performance and actions towards preventing another incident and making sure they respond appropriately if there is in fact another incident (Cassetto, 2022).

References

1) *Business Continuity Plan | Ready.gov*. (n.d.). https://www.ready.gov/business-continuity-plan

2) Cassetto, O. (2022, September 19). *Incident Response Plan 101: The 6 Phases, Templates, and Examples*. Exabeam. https://www.exabeam.com/incident-response/incident-response-plan/

1) Disaster Recovery Plan

a) Response Phase:

i) In the event of a natural disaster like a tornado, fire, or earthquake the IT response team shall make sure that the impacted system is cleaned up in making sure that any security holes that may exist are closed. Make sure to recover current data as this will be detrimental in the recovery phase that should be done every day around 2:00 pm EST to the backup site at 123 east main street, Thornville, Mississippi.

b) Recovery Phase:

i) Data

(1) In the event of data loss, the IT response team should try and recover as much current data as possible from the damaged site using EaseUS Data Recovery Wizard as the hard drives are windows based and will be able to recover some of the data if not all so the company can recover more promptly (1). Pending the current data recovery, the backup site as mentioned above will take over the current load from the web page and get the company back up and running. This will require the response team to make sure that the backup site is fully functional, and that all hardware is in full working condition, so the company does not lose more than it already has. To get the company up and running after the disaster the response team allocated for current data collection will go to the main site and the ones allocated for getting the warm site up and running will do so.



c) Resumption Phase

i) Here the company will pick up at the warm site pending on who may be able to come to work. This will be followed by the IT response team ensuring that all hardware and backup drives are functioning properly and the recovered data is restored to the system by the data recovery response team. This will be followed by the designated employees reporting to the warm site to resume business under restricted business operations. This will also include the designated employees and staff letting the customers know about the incident and letting them know to expect longer than usual wait times for call-ins and web page access. Along with notifying vendors of the implications and that the company will be under restricted functionality for no longer than a month pending damage assessment and repairs.

d) Restoration Phase

i) Repair and Replacement

(1) Repair

(a) After Resumption Phase is underway, the main site recovery team will undertake to get the main site up and running again. This will involve assessments of the damage, followed by a damage assessment and what will be required to get the main site for the company back up and running at full capacity. This will take about a week to complete followed by the assessment and the necessary building damage needing repairs along with the hardware.



(2) Replacement

(a) Following the proper assessment is completed and the proper contractors for building and hardware replacements are made the process should start with any building repairs, followed by all and any hardware repairs and

replacement. This will include a final inspection to include but not limited to all safety inspections and functional checks that will intel the final checks of the main site and that it is fully operational.

References

1) *Professional data recovery software to restore formatted or deleted files, corrupted drives or any inaccessible data - EaseUS Data Recovery Wizard.* (n.d.). https://www.easeus.com/ppc/data-recovery-bing.html?ad