**RISK MANAGEMENT FOR**

**INSTAGRAM FOR BUSINESS**



**The Bomb Squad**: Bhargav Sabbineni, Ipsa Ojha, Jeremiah Warren, Kaustuv Dutta, Swati M. Radia

**Table of Contents**

[**Executive Summary** 3](#_Toc121237702)

[**Background** 3](#_Toc121237703)

[**Attacks** 6](#_Toc121237704)

[**Instagram for Business** 9](#_Toc121237705)

[**Our Scenario** 10](#_Toc121237706)

[**Assets** 12](#_Toc121237707)

[**Threats** 12](#_Toc121237708)

[**Weighted Factor Analysis – Assets** 12](#_Toc121237709)

[**Weighted Factor Analysis – Threats** 13](#_Toc121237710)

[**Threat Vulnerability Assessment** 14](#_Toc121237711)

[**Risk Calculation** 14](#_Toc121237712)

[**Cost Benefit Analysis** 15](#_Toc121237713)

[**References** 16](#_Toc121237714)

[**Exhibits and Appendices** 17](#_Toc121237715)

# **Executive Summary**

Social media has influenced almost every aspect of human life in the 21st century. Humans not only use social media to communicate and share information, but we also use these platforms to build brands and drive organizational growth. While the commercial potential of social media may be endless, social media does not come without risk.

For our case, we have chosen to examine the risk associated with Instagram, the popular image and video sharing site. We begin our analysis with a comprehensive history of Instagram’s rise, with a particular focus on how Instagram evolved to be a platform for business. Following this chronology, we examined some of the instances of data breaches and account hacking experienced by Instagram and its users. This section further highlights the risks associated with this platform and drove our risk assessment process. Then we analyze the growth of Instagram’s Instagram for Business platform, which allows organizations to market and sell products to Instagram’s massive user base.

After focusing on Instagram as a whole, we decided to create a fictional small business called Painted that relies on Instagram for a majority of its sales. Conducting a risk assessment based on this fictional scenario allowed us to further explore some of the previously identified risks. We began our risk assessment of Painted, our fictional company, by cataloguing the company’s threats, assets, and vulnerabilities. Then we determined our most critical assets and threats and calculated the risk associated with each threat. Finally, we conducted a cost-benefit analysis of two possible controls for our most critical threat.

# **Background**

We begin our analysis with a summary of how Instagram came into being and steadily evolved over the years before delving deeply into the complexities of the business model used by Instagram to produce huge revenue. Instagram is currently valued at $100 billion.

Instagram, one of the most widely used social networks worldwide, was introduced by Kevin Systrom and Mike Krieger in 2010. Facebook acquired Instagram for a then-unprecedented $1billion in April 2012. At the time of the acquisition, Instagram was growing fast, but it had only 25 million registered users, minuscule compared to Facebook’s hundreds of million users. To top it off, Instagram was not bringing in any revenue; it was being run by 13 employees.

Even Twitter took its shot at courting Instagram before Facebook finalized the acquisition. However, Kevin Systrom and Mike Krieger, the creators of Instagram, opted to continue working with Facebook because, in addition to the enormous quantity of money, Zuckerberg also held out the prospect of independence.

Instagram would be given the opportunity to continue operating as a separate business if it agreed to be acquired by Facebook. This would allow Instagram to not only avoid the security issues, but it helped to gain access to Facebook's engineering experience. Independence would soon wane, though, and was a major factor in both creators of Instagram leaving Facebook.

After the acquisition, Instagram’s monthly active user count kept growing. More than 500 million active users were using Instagram by June 2016. And Instagram touched 1 billion monthly active users in June 2018, before the Instagram founders resigned towards the end of 2018 owing to irreconcilable differences and gradual erosion of autonomy.

**Here is a chronology of how Instagram evolved over time:**

**2012:** Facebook acquires Instagram in April 2012. This is major news and has a large impact on Instagram's development.

**2013:** Instagram now permits links to videos hosted on other websites. Brands' engagement is increased because of these integrated links. Michael Kors, the first authorized user of Instagram, gains 34,000 new followers in just 18 hours after the platform launches sponsored post advertising in November 2013.

**2014:** In response to the popularity of sponsored posts, Instagram introduces the business profile. Although this new feature had some limitations, Facebook's tools allowed for the incorporation of a dashboard interface for the analysis of impressions, reach, and frequency in relation to advertising campaigns and specific ads.

**2015:** CTAs are made available! In anticipation of sales, Instagram introduced additional conversion kinds like app installs, email sign-ups, and links to shop websites. They also hint at additional targeting options based on Facebook's detailed user information.

**2016:** Instagram Stories were introduced. Photos and videos can be updated in Stories for an entire day. This is essential for business interaction because it enables businesses to give their customers an intimate look behind the scenes. Since then, 37% of all impressions for businesses have come via Instagram Stories.

**2018:** New communications can now be shown in the direct inbox of business accounts. They also incorporate prompt responses to lessen the pressure. Instagram Stories can now include links. Since customers can navigate directly to a specific product page, using this functionality has become essential. Business-related Stories account for one-third of the most popular Stories. Now that businesses may add product stickers to Stories, users can do so more easily.

**2019:** Instagram introduces an in-app payment function that enables users to make purchases within the Instagram app rather than on an external website. This function paved the way for several shopping-related enhancements that have elevated Instagram to a significant position in the e-commerce space.

**2020:** Instagram includes a secondary inbox option for business profiles. Businesses can categorize their direct communications into low priority and high priority using the new inbox. Instagram launches several stories and profile features to aid small companies in response to the COVID-19 pandemic. The Instagram app allows business pages to add "stickers" to their stories that allow users to donate money, buy gift cards, or place food orders. Additionally, these buttons may be immediately added to the company profile. Instagram also launched a feature that allows creators to tag and promote products within their Live videos as a result of Instagram Live's viewership increasing by 70% during the first month of the epidemic.

Facebook releases the Facebook Business Suite app in October 2020, formerly known as the Pages Manager App, enabling small businesses to manage their content, communications, and statistics for Facebook and Instagram in a single location. Product tags for advertisements officially launch. In Instagram advertisements, users may click on tags to discover product information, prices, and to make a purchase.

**2021:** Instagram introduces a Professional Dashboard for businesses and creators that offers metrics, insights, and tools from within the Instagram app.

# **Attacks**

Before we created our scenario, we investigated several instances of data breaches experienced by Instagram and its users. Here are some of the more interesting stories that we found:

**Data Leak in January 2021 Discloses Scraped Information on 214 million Social Media Accounts**

A significant data breach at SocialArks in January 2021 compromised 318 million records, encompassing over 214 million social media accounts. The breach was caused by a poorly designed database. Without a password, information could be accessed, and the data within wasn't secured. Anyone who could connect might therefore see the whole contents of the data storage. Many account holders' personal information was contained in the leaked database. The collection also included some users' phone numbers and email addresses in addition to profiles, follower counts, and other comparable information.

The database concentrated on material that had been "scraped," or compiled from publicly available data by a business, organization, or individual. To produce more complete records for certain persons, businesses, or entities, some database developers of scraped information aim to reconcile information they gather across numerous platforms in addition to collecting individual pieces of data.

The business that obtained the information was within their rights to do so since web-scraping is not inherently unlawful. Additionally, nothing is compromised during scraping. At the time of collection, all the data was accessible on the original platform.

The majority of social networking networks' rules and conditions prohibit scraping, nevertheless. That applies to Instagram, Facebook, and the majority of other widely used social media platforms.  
   
**235 million Social Media Profiles Will Be Revealed by a Large-Scale Data Breach in August 2020**

In August 2020, it was discovered that an unencrypted database had 235 million YouTube, TikTok, and Instagram profiles. the database administrators were informed that the data was not sufficiently safeguarded and was essentially readable by anybody who found the data cache.

The available data included a variety of personal details. While some records also included email addresses and phone numbers, the bulk of the data just included full names, genders, ages, and profile pictures.  
   
Deep Social, a third company that gathered information by scraping information from accounts, had amassed the data. Deep Social closed its doors in 2018 when Facebook forbade it from harvesting user information from Instagram profiles and threatened legal action. Many people were unsure of how long the information had been accessible to the public because Social Data, another firm, was managing the database.

**49 million records were exposed in the Chtrbox database in May 2019.**

A sizable database run by a third-party business was uncovered online in May 2019. An inadequately guarded Amazon Web Services server managed by Chtrbox, a business that compensated influencers for sponsored postings, allowed the exposure of this data. The information may be accessed without a password because the data wasn't encrypted.  
Personal contact information, such as email addresses and phone numbers linked to accounts, as well as account information like follower counts, locations, and more were contained in the records.

The data also included information on the accounts' projected worth. Since the company dealt in sponsored posts, it used statistics on reach, follower counts, engagement rates, and other factors to estimate how much each account would be worth, thereby giving the profiles a monetary value.  
   
It is crucial to remember that the first data breach claims indicated that a startling 49 million records were exposed. Chtrbox refuted the claim, claiming that the event only had the potential to affect 350,000 influencers. It's not entirely clear how many people were impacted.

**March 2019: Unencrypted Storage of Hundreds of Millions of Passwords.**

Facebook revealed in March 2019 that it had unintentionally saved hundreds of millions of user passwords in an unencrypted format. These passwords belonged to accounts on Facebook, Facebook Lite, and, as the business disclosed in April, Instagram accounts.

Within the firm, these passwords were freely accessible. Companies typically only save encrypted passwords in order to safeguard this data in the event of a cyberattack. In the case of Facebook, these passwords were readily accessible for many years.

**Contact information for 6 million account holders was compromised in August 2017**

6 million Instagram accounts were affected by a data breach that became public in August 2017. A flaw in the Instagram developer API made it easy to extract email and phone information about Instagram accounts from the website. Instagram fixed the problem, although it didn't seem to happen in time.

Hackers published a website with a searchable database that purportedly contained the personal contact information of prominent users. The gang allegedly began concentrating on accounts with more than a million followers before moving on to other accounts. In the end, it seemed that both famous people and everyday individuals were included in the data. The hackers demanded a fee for each search before selling the information for Bitcoin.

Following the incident, Instagram contacted verified accounts to let them know about the breach.

**InstaAgent App Caught Stealing Passwords in November 2015**

InstaAgent, a third-party Instagram client, was found to have been harvesting and sharing Instagram usernames and passwords without the owners' consent in November 2015, according to Apple and Google.

After the event, Instagram tightened restrictions on third-party apps and severely limited access to its API.

We couldn't uncover any prior reports of Instagram data breaches. However, throughout the years, its parent firm has also seen its fair share of data breaches and privacy abuses.

# **Instagram for Business**

With Instagram’s growing popularity, more services are being added to Instagram. Back in November 2013, Instagram introduced sponsored posts to advertise products. The first sponsored post was from Michael Kors, which helped the brand gain 34,000 new followers in only 18 hours. Many businesses saw this as an opportunity and started having sponsored posts to get more followers and in turn more customers buying their product.

Instagram launched the business profiles in August of 2014 after seeing the huge popularity with sponsored posts. Soon after all the major companies and brands started converting their page into business page. As per Instagram statistics there are about 200 million business accounts as of 2022. Around one-third of the most viewed Instagram Stories are posted by businesses. This shows that businesses pages are getting a lot of popularity and attention.

Businesses of any size can create their Instagram business accounts and reach millions of users across the world. There are only a few simple steps to follow to create and set up an Instagram business account. This means small to medium sized business can start without having to invest a lot in marketing and Instagram helps them with exactly that. All the business owners must do is start posting their products and make their business page interesting so that more users begin following.

Initially when business accounts were introduced by Instagram, it was necessary to create a Facebook business page and then link to with Instagram account. Now, users can convert their Instagram account to a business page without having a Facebook page. Then the business owner can start posting about their products via images, video or even make reels, (short videos introduced by Instagram to compete against TikTok) which are gaining a huge momentum. Users can shop by accessing the website link that is usually posted in the account bio (brief summary of the business page).

Another way to shop using Instagram is using the latest service launched by them in 2020, Instagram shop. Facebook previously had an app called Pages manager app which they revamped to be Facebook Business Suite App. This app helps businesses to manage their content, messages, and analytics in one place. This suite of apps can be accessed using the website [business.faceboook.com](https://business.facebook.com/). The user must first create an account in Facebook business suite app and link their Instagram or Facebook business pages.

The app helps to set up payment methods using either of these three options. First, using checkout with another website, which links to the business/ product website. Second, checkout with Facebook or Instagram. Lastly, using checkout with messaging. Once the payment method is selected, the business owner can go on to add product catalogues. After having added all the products in the catalogue, this new catalogue must be added to the Instagram business account.

The business owner can then login into the Instagram business account and choose settings. Then choose the option to set up Instagram shop. Link the newly created product catalogue and verify the website domain and complete the process. Then on the business account owner can add posts with tagged products, which gives details of the products and price. Customer can then directly shop from Instagram.

Business owners can choose to have ads for their products as well. These ads will randomly pop up on user profile as they scroll through their feeds. These ads pop up based on the AI (Artificial Intelligence) models developed by Instagram. This helps to get more users and followers and hence helps in marketing. Instagram charges higher cost per click compared to Facebook, Therefore Instagram ads are costlier. It can cost between $0.20 to $2.00 per click to run an Instagram ad campaign.

# **Our Scenario**

Painted is a clothing boutique selling customized clothing. The company was founded by two friends in 2018, and it became popular when Painted’s designs went viral on Instagram during the pandemic. In 2020, the company decided to shift its business model to focus on sales through Instagram’s Instagram for Business platform, and now 60 percent of the company’s sales come from the company’s Instagram shop, with the other 40% coming from company’s website. Currently, the company has five employees, the two founders and three other full-time employees. The two founders design and produce the company’s clothing. Of the three other employees, one handles the company’s IT infrastructure, one handles sales and marketing, and the other is tasked with handling shipping and logistics. Painted’s employees all work in a company-owned warehouse that has been converted into a design studio and office. The company’s IT infrastructure consists of a company laptop for each employee, the company’s website, and servers. Painted has a web server, a database server, a mail server, and file server.

Although Painted is a small operation, they have experienced numerous attacks during the last year, including denial-of-service attacks, their company accounts being hacked by malicious attackers, phishing attacks, and an insider threat attack. They experienced two DOS (denial of service) attacks this year, which took down their company website for four hours each time. While Painted’s company website was down for four hours during the DOS attack, they missed out on approximately 40 orders of around $50 each, costing the company $2,000 for each occurrence. After their company’s accounts were hacked, the attackers were able to change Painted’s payment settings and redirect customer payments to a bank account controlled by the attackers. Each time this happened Painted lost $1,000 in customer payments. Painted was also the victim of 4 successful phishing attacks, costing the company a total of $3,000. The costliest of the attacks experienced by Painted came from a disgruntled former employee. This employee sold company data about the launch of a new line of products that was projected to be extremely popular to a competitor. This attack cost the company $10,000.

Painted is considering controls to address each of the attacks they experienced this year. To address the denial-of-service attacks, Painted is considering several firewalls that will cost the company approximately $750 annually. Painted expects the firewalls to mitigate the risk of DOS attacks by 20%. In order to prevent their company accounts from being hacked again, Painted is considering implementing multi-factor authentication for all of their company accounts. To implement multi-factor authentication on their company accounts, all of Painted’s employees would be either be issued an iPad or an RSA token. Each iPad would cost the company $350, and it would mitigate the risk of hacking by 50%. The RSA tokens cost $300 each and mitigate the risk of hacking by 60%. To combat the phishing attacks experienced by the company, Painted is considering a $600 security training course for staff that will mitigate the risk of this form of attack by 25%. To mitigate the risk of insider threats by 70%, Painted is considering employing RBAC (Roles Based Access Control) controls by moving their services to AWS (Amazon Web Services) or using an IAM (Identity and Access Management) product from Okta. These options would cost the company approximately $500 per year.

# **Assets**

Our analysis identified the following assets for Painted: IT infrastructure (consisting of the four servers and the company website), Instagram profile, company reputation, company staff, company warehouse, and company laptop (See Exhibit 1).

# **Threats**

In our scenario, Painted faces the following threats: denial-of-service attack, accounts being hacked, phishing attacks, and insider threat (See Exhibit 1).

# **Weighted Factor Analysis – Assets**

For our weighted factor analysis, we chose to evaluate our assets using the following criteria: Impact on Revenue, Most Critical for Success, and Impact on Public Image. We assigned weights of 35% to Impact on Revenue and Impact on Public Image and 30% to Most Critical Success (See Exhibit 2). Since Painted is a small business, we decided that impact on revenue needed to be one of the most important criteria in our analysis. We thought that any change in revenue might jeopardize the viability of the company. Because Painted is a small business that is reliant on social media, its public image is critical to the company, so we allocated an equal percentage to Impact on Public Image. While we thought evaluating Painted’s assets by how critical they were to the company was important, we allocated slightly less weight to this criterion in our evaluation.

After completing our weighted factor analysis, our assets ranked in order of descending importance are reputation of the company, Painted’s business Instagram profile, the company warehouse, the IT infrastructure of the company, the company’s staff, and staff laptops. The two most important assets, Painted’s reputation and its Instagram profile, were allocated considerable weight under each criterion. We ranked the importance of the company’s reputation the highest in the Impact on Public Image category, which reflects our belief in the importance of public image to a small business operating on social media. Since the Painted’s Instagram Profile is critical to the company, it received high weights across all of the criteria. We ranked several of the others highly but slightly less important as our top 2 assets. And finally, we ranked the company’s laptops as the least important asset, because we believed that if something were to happen to the laptops, we thought that they could be quickly replaced (See Exhibit 2).

# **Weighted Factor Analysis – Threats**

For our weighted factor analysis, we chose Probability of Success, Cost to Protect, and Financial Loss if Successful as our criteria for evaluating the threats facing Painted. Since all of our threats are costly to Painted’s bottom line, we chose Probability of Success and Financial Loss if Successful as our two most important criteria. Again, we allocated slightly less importance to our third criterion, thinking that our controls would cost less than the attacks themselves. This ranking reflects the importance we assigned to Painted’s bottom line (See Exhibit 3).

According to our weighted factory analysis, Painted’s threats, in order of significant, are their company accounts being hacked, phishing attacks, insider threat, and DOS attacks. Accounts being hacked was our biggest threat by a wide margin, as this threat received high scores across all the criteria. Account hacking happened the most frequently of the last year, cost the second most of all the threats in total, and would cost the most to protect against. While the insider threat was the costliest to the company in terms of impact, it only happened once last year, which is reflected in the weights we assigned to it. DOS and phishing attacks received similar scores across several of the categories, but the frequency of the attacks proved to be the differentiator (two DOS attacks, as opposed to four phishing attacks). (See Exhibit 3).

# **Threat Vulnerability Assessment**

Threat vulnerability assessment is a process of listing all the assets and the threats and assessing which vulnerability will threaten the corresponding asset. For our threat vulnerability assessment, we considered all the assets and threats we listed in the previous section (See Exhibit 4). We listed a few of the vulnerabilities that could be exploited by the threats. Not having a strong security policy for IT infrastructure could possibly result in a denial-of-service attack. Hence, it is very important for the organization to have a strong firewall, intrusion detection and intrusion prevention systems.

Social media accounts need to be protected using strong passwords, turning on multi factor authentication or even having a good access control for the employees. If any of these are not set up, this could result in threats like account being hacked and insider threat. To avoid social engineering threats like phishing, the organization needs to invest in a good security training program of the employees. This will help in protecting IT infrastructure.

All the employees of the company have a laptop, and they also have a warehouse for their products. There needs to be good physical security in the office/warehouse location, if not this may result in theft. (See Exhibit 4).

# **Risk Calculation**

Risk calculation considers the impact, likelihood, percentage mitigation and the percentage uncertainty of the threat. For the purpose of calculation, the considerations we made are, impact to be the cost incurred by a certain threat. The number of times a threat occurred in a year divided by the total number of all the threats is the likelihood of each threat. We considered mitigation to be the percentage of the reduction in a possible attack that the current controls provided. Percentage uncertainty is assumed to be 10% for all the threats.

Based on the consideration and assumptions, we calculated the risk for each threat using the risk calculation formula i.e. (See Exhibit 5) for all the calculations.

**Risk = (Impact x Likelihood) - % Mitigation + % Uncertainty**

After calculating risk for all the threats, Account Hacking resulted with the highest value for risk.

# **Cost Benefit Analysis**

Cost Benefit Analysis (CBA) is the process which organizations use to compare the costs and benefit associated with a decision to determine if it is feasible or not.

**CBA = ALE(precontrol) - ALE(postcontrol) - ACS**

ALE(precontrol) is the annualized loss expectancy of the risk before the implementation of the control

ALE(postcontrol) is the annualized loss expectancy examined after the control has been in place for a period.

ACS is the annual cost of the safeguard.

Based on the risk assessment we found that account hacking is the most important risk for which we need to implement controls. So, we perform CBA for its control which is multi-factor authentication. It can be achieved in 2 ways, first by providing each employee with an iPad or second, by issuing an RSA token to each employee. Based on the calculations, we conclude that Painted should go with iPad as the control. Since the CBA value is higher for iPad than RSA (See Exhibit 6).

# **References**

Instagram Business  
[**https://business.instagram.com**](https://business.instagram.com/)

Brief history of how Instagram features have evolved [**https://www.perfectsearchmedia.com/blog/brief-history-how-instagram-s-business-features-have-evolved**](https://www.perfectsearchmedia.com/blog/brief-history-how-instagram-s-business-features-have-evolved)

How Instagram makes money  
[**https://whatisthebusinessmodelof.com/business-models/how-instagram-makes-money/**](https://whatisthebusinessmodelof.com/business-models/how-instagram-makes-money/)

Instagram business model canvas  
[**https://vizologi.com/business-strategy-canvas/instagram-business-model-canvas/**](https://vizologi.com/business-strategy-canvas/instagram-business-model-canvas/)

Instagram business model  
[**https://www.apptunix.com/blog/instagram-business-model/**](https://www.apptunix.com/blog/instagram-business-model/)

Case study: How my business Instagram was hacked  
[**https://www.mybusiness.com.au/resources/news/case-study-how-my-business-instagram-was-hacked**](https://www.mybusiness.com.au/resources/news/case-study-how-my-business-instagram-was-hacked)

Instagram Hack Bigger Than Thought

[**https://www.pymnts.com/news/security-and-risk/2017/instagram-cyberattack-larger-than-thought/**](https://www.pymnts.com/news/security-and-risk/2017/instagram-cyberattack-larger-than-thought/)

# **Exhibits and Appendices**

**Risk Analysis**

|  |  |  |  |
| --- | --- | --- | --- |
| **Assets** | **Threats** | **Vulnerabilities** | **Controls** |
| * IT Infrastructure (Servers, Company Website) * Customer PII * Instagram Profile * Reputation * Company staff * Warehouse * Company Laptops (Hardware) | * DOS * Account Hacking * Phishing Attacks * Insider Threat | * Patching Issues * Weak Credentials * No MFA * Relying on nonefficient third party * Undertrained customers or employees | * Firewall * Multi Factor Authentication (MFA) * Security trainings for staff * RBAC |

Exhibit 1

**Weighted Factor Analysis – Assets**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***List|Criteria*** | **Impact on revenue - 35%** | **Most Critical for Success – 30%** | **Impact on public Image – 35%** | **Total** |
| **IT Infrastructure (Servers, Company Website)** | 90 (31.5) | 70 (21) | 50 (17.5) | 70 |
| **Instagram Profile** | 70 (24.5) | 80 (24) | 75 (26.25) | 74.25 |
| **Reputation** | 75 (26.25) | 60 (18) | 90 (31.5) | 75.75 |
| **Company Staff** | 30 (10.5) | 75 (22.5) | 10 (3.5) | 36.5 |
| **Warehouse** | 80 (28) | 80 (24) | 60 (21) | 73 |
| **Company Laptops (Hardware)** | 30 (10.5) | 20 (6) | 10 (3.5) | 20 |

Exhibit 2

**Weighted Factor Analysis – Threats**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **List|Criteria** | **Probability of Success**  **35%** | **Cost to Protect**  **30 %** | **Financial Loss if Successful- 35%** | **Total** |
| **DOS** | 20 (7) | 40 (12) | 45 (15.57) | 34.57 |
| **Account Hacking** | 80 (28) | 90 (27) | 80 (28) | 83 |
| **Phishing Attacks** | 60 (21) | 30 (9) | 35 (12.25) | 42.25 |
| **Insider Threat** | 10 (3.5) | 20 (6) | 90 (31.5) | 41 |

Exhibit 3

**Threat Vulnerabilities Assessment**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threats/ Assets** | **IT Infrastructure (Servers, Company Website)** | **Instagram Profile** | **Reputation** | **Company Staff** | **Warehouse** | **Company Laptops (Hardware)** |
| **DOS** | Weak security policy (no firewall) |  |  |  |  |  |
| **Account Hacking** |  | -Using poor credentials -No MFA | -Using poor credential -No MFA |  |  | Weak password policy |
| **Phishing** | Filtering external emails |  |  | Lack of security training |  |  |
| **Insider Threat** |  |  |  | Lack of RBAC |  |  |
| **Theft** |  |  |  |  | Lack of physical security | Lack of physical security |
| **Priority of Controls** | 4 | 2 | 1 | 5 | 3 | 6 |

Exhibit 4

**Risk Calculation**

|  |  |  |  |
| --- | --- | --- | --- |
| **DOS**  Likelihood = 0.166  Impact = $4,000  Mitigation = 20%  U% = 10%  R = (L x I) – M% + U%  R = (0.166\*4000) - 20% +10%  R = (664) -1 0%  R = 664 – 66.4  R = **597.6** | **Accounting Hacking**  Likelihood = 0.416  Impact = 5000  Mitigation = 50%  U = 10%  R = (0.416 \* 5000) - 50% +10%  R = (2080) -( 40% of 2080)  R = 2080 –832  **R = 1248** | **Phishing**  Likelihood = 0.333  Impact = 3000  Mitigation = 25%  U=10%  R= (0.33\*300) - 25% + 10%  R = (990) -15%  R= 990 – 148.5  **R = 841.5** | **Insider Threat**  Likelihood = 0.08  Impact = 10000  Mitigation = 70%  U = 10%  R = (0.08 \* 10000) - 70% +10%  R = (800) - (60% of 800)  R = (800 – 480)  **R = 320** |

|  |  |
| --- | --- |
| **Risk Calculations [R = (L\*I) -M% + U%]** | |
| DOS | 597.6 |
| Account Hacking | 1248 |
| Phishing | 841.5 |
| Insider Threat | 320 |

Exhibit 5

**Cost Benefit Analysis**

ALE (Annualized Loss Expectancy) = Single Loss Expectancy \* Annualized rate of Occurrence

CBA (Cost Benefit Analysis) = ALE (pre-control) - ALE (post-control) - ACS

Assumptions:

1. iPad – 5 for 350

Reduction to SLE 50%

1. RSA – 300$ for each RSA token

Reduction to SLE 60%

|  |  |
| --- | --- |
| **iPad** | **RSA** |
| ALE (pre-Control) = 1000 \* 5 = 5000  ALE (post Control) = 500\*5 = 2500  ACS = 5 \* 350 = $1,750  CBA = 5000 – 2500 – 1750 = 750  **CBA = 750** | ALE (post Control) = 600 \* 5 = 3000  ACS = 5 \* 300 = 1500  CBA = 5000 – 3000 – 1500 = 500  **CBA = 500** |

Exhibit 6