University of Louisville

Social Media: Privacy and Security

Addison Phillips

CIS 481-50-4225

Professor Wright

08/09/2022

Table of Contents

[Executive summary 3](#_Toc110785345)

[Introduction 4](#_Toc110785346)

- Why social media is relevant to businesses

[Overview 4](#_Toc110785347)

- Fraud accounts

- Phishing attacks

- Damage to Reputation

- Unauthorized user attacks accounts

- Distribution of confidential information

[Problem 1: Damage to Reputation 7](#_Toc110785348)

- What it is and how reputation is damaged

- Why it poses a threat to businesses. (Money, fame, etc.)

- Previous examples of this with companies and the impact of the damaged reputation

[Problem 2: Distribution of Confidential Information 10](#_Toc110785349)

- What is confidential information and how can it be used as a threat against companies

- Social media policies

- Why privacy and security are important and unique to each company

- Threat of employees: venting online, falling for social engineering and profile cloning, and victims of phishing attacks

[Solution for Healthcare Companies 13](#_Toc110785350)

- Emphasis on confidentiality

- HIPAA compliance

- Controls/solutions

[Solution for Logistic Companies 16](#_Toc110785351)

- The importance of protecting logistic information

- Addressing security risks

- Controls/solutions

[Conclusion 18](#_Toc110785352)

[Works Cited 20](#_Toc110785353)

# Executive Summary

As more and more businesses interact with customers and build their images on social media apps, it becomes more important to safeguard against threats on social media. Some of these threats include phishing, fraud, damage to reputation, and distribution of confidential information with the latter two being the focus of this report. Damage to a company's reputation can result in numerous consequences such as financial loss, lower retention of employees, and potential penalties or fines. The distribution of confidential information can tarnish a company's reputation but also violate many legal and ethical standards specific to the industry it occurs in. Social media can greatly impact a business for better or for worse which is why there needs to be a great deal of focus on the threats to information security and privacy on social media.

The way an organization handles and prioritizes these threats can be unique from industry to industry. Some industries have a specialized set of standards or rules that must be followed when it comes to keeping information confidential. For example, organizations in the healthcare industry must abide by HIPAA. This is a federal law that mandated the creation of national standards in order to protect sensitive patient health information from being distributed without the patient being aware or consenting to it. Meanwhile, other industries such as the logistic industry must focus more on ethical standards and maintaining a good reputation. In both cases solutions must be implemented to prevent any damage that may come from the use or misuse of social media.

The solutions, safeguards, and policies organizations implement from industry to industry regarding social media are similar. The root cause of all harm done to organizations on social media can be traced back to people. Because of this, the focus must be on employee awareness and training on the use of social media. Educated employees result in the proper handling of social media and the reduced chance of attacks through social media that try to manipulate employees into giving up sensitive information in being successful. There must be social media policies in place in every type of organization. The employees working there must be required to review these policies and comply with them in order to stop the spread of confidential information and tarnish the reputation of a company. Although not all attacks and threats to an organization can be stopped permanently, there can and should be controls implemented to stop as many as possible.

# Introduction

Social media has become a mainstay in the operations of businesses around the globe. It allows them to maintain a positive public image while strengthening bonds with consumers. These consumers trust businesses to handle their personal information and keep it secure from any threats that may arise. Therefore, it is the business’s priority to make sure all information is protected with the implementation of safeguards and controls. When dealing with protection, it is integral to distinguish the differences between privacy and security. Privacy is the handling of data and the emphasis on proper use, while security is the protection of data from outside threats. The key difference in these terms is the people acting on them. Typically, employees are made aware of the need to maintain the privacy of information, while security focuses on individuals who are outside of the organization. Employees can use their social media platforms to discuss work with colleagues, presenting an issue of security. Other issues facing organizations arise from outsiders who can ruin reputations by slandering an organization's name and/or operations.

Many companies use social media accounts to promote their business and maintain client relationships, so it is imperative they keep a clean reputation online. With damaged reputation comes fallen sales, lower employee retention, hardships recruiting new talent, and an overall loss in money. By having a damaged reputation, businesses take massive hits in public relations which are detrimental to the scale of the company. Distribution of confidential information is an issue that more companies are starting to face, leading to privacy breaches and accidental misuse of technology by employees. Every company is tasked with developing solutions to combat security and privacy issues. Healthcare and Logistics companies are among some of the most influential companies in today’s world, and each is responsible for finding solutions regarding privacy and security that work best for their unique needs. In healthcare and logistics businesses, different violations are at risk of being committed – such as HIPAA. The solutions proposed here can help control the various social media attacks and concerns.

# Overview

Social media is a massive part of the modern world – in fact, 82 percent of Americans have at least one social media account, which in turn equates into 223 million social media users in the United States alone. This is a huge jump from 10 years ago, when only 52 percent of the country’s population had a social media account (Dixon). Unfortunately, this heightened usage of social media can, and has, translated into other issues. Social media collects a lot of personal data for everyone that signs up – and if personal accounts fall into the wrong hands, data breaches and confidentiality breaches can occur. One of the top issues that companies face in a modern, highly technological world is the issue of confidentiality – employees are key information-holders in corporations, so they too must uphold a standard of privacy in order to protect their company’s confidential information. Consider the following situation: You are having a conversation on Facebook with your coworker regarding future releases the company is having, along with some other confidential information. You continue to have work-related conversations with this individual, discussing internal company matters – but it's just between the two of you. Now, consider if you happen to be one of the 533 million Facebook users whose personal data was leaked online – for free (Nexstar Wire). Those conversations that you had privately may no longer be private – and the information that was in your conversation could very well be available to anyone who’s seeking it.

Let’s examine another situation. In 2010, an individual in the Israeli military updated his Facebook status – but, in doing so, he exposed both the location and the time of an upcoming raid, which then led to the Israeli military having to cancel the entire operation (McGregor-Wood). This is just one very real example of many situations where confidential information is leaked, and unintended consequences follow. These simple mistakes go hand-in-hand with a modern form of manipulation – social engineering. The definition of social engineering is the “act of exploiting human weaknesses to gain access to personal information and protected systems.”[[1]](#footnote-2) This form of exploitation relies on human error more than anything else, and social media sites tend to be a huge magnet for social engineers due to the large amount of personal data that is publicly available (Kenton). The first example of this is the usage of fraudulent accounts by malicious individuals. These fraudulent accounts can be used to pose as a banking institution, work-related resources, or even a friend – and they try and manipulate the victim into giving out personal information that they would normally give to a trusted individual, or institution. For example, if you’ve ever been reached out to on social media by an unknown account asking you to click a link or provide personal information, you’ve been targeted by a fraudulent account.

Another example of exploitation that can occur on social media is phishing. As defined by Cisco, a phishing attack is defined as “counterfeit communications that appear to come from a trustworthy source, but which can compromise all types of data sources.”[[2]](#footnote-3) This is one of the biggest threats against organizations as their employees are often targeted in phishing attacks through counterfeit emails or direct messages that contain links that procure personal data which are then used to hack into internal systems *(What is Phishing*?). This type of attack is extremely common, but also very avoidable as long as proper training is given to all employees. It is worth the investment for companies to train on common attacks such as this one – according to the Cost of Phishing Study, in 2021, the annual cost of phishing attacks alone was $14.8 million for large corporations. This includes the money spent on fixing infected systems, credential compromises, and loss in employee productivity as efforts are diverted towards repairing the damage done from the attack (SC Magazine).

Social media has given everyone a voice online – and these individuals voice both positive and negative views – whether they be good or bad. Take the art director at Lululemon, who in 2020 reposted a link to a shirt on his personal Instagram page. This shirt contained offensive images that carried underlying racism against Asian-Americans. This post made by a single employee caused an uproar online, many claiming that they would boycott the corporation out of disagreement with the employee’s views. Lululemon had to quickly respond and posted a formal apology, along with firing the employee involved (Hanbury). Although the post was not made on any official company accounts, the post by the employee did some serious damage to their public relations, and in turn, cost the corporation money. There is a plethora of examples just like the one given above – companies’ reputations damaged by employees who post carelessly on their personal accounts. Nowadays, many companies have a social media policy, or make strong encouragements or suggestions for employees as to how to conduct themselves online, especially because they often associate themselves with their workplace online in one way or another. These social media policies protect both the employee and the employer – the guidelines make it clear what is acceptable and what is not, and in turn, the employer is more likely to avoid a public relations disaster.

Today, even with the complexity of different cyber-attacks that occur online, the leading cause of breaches continues to be unauthorized user access. Often times, this is caused by simple mistakes, such as reusing passwords, using easy-to-guess passwords, or not securing personal information. These basic failures can lead to catastrophic consequences, giving unauthorized individuals access to highly sensitive user and company information (Molok). The average costs of these breaches fall to about $8.64 million – a costly mistake with a simple solution. Healthcare is the most targeted industry for these attacks, accounting for 34% of these attacks, as cybercriminals try to extort money in exchange for the stolen information (HelpNet Security). Corporations have made changes to their security policies in order to try and avoid these breaches, such as enforcing longer passwords, consistent password changes, and harder to crack authentication methods, such as two-factor authentication. These simple practices make it significantly harder for cybercriminals to access sensitive information, and in turn, keep the employees, customers, and corporation safer.

Lastly, all these attacks and vulnerabilities combined lead into one large, universal, issue – the issue of unauthorized distribution of confidential information. The different types of problems mentioned above all end up divulging sensitive information in one way or another, and in these cases, they’re falling into the wrong hands. The amount of damage that is done each year due to these privacy failures is massive, and ultimately, we believe that there are appropriate and effective ways to address these issues. Although the issues that are faced for each sector differ, there are still universal guidelines that can be put into place to safeguard information and data in the modern world. We will investigate these universal issues further, and dive into specific problems and their associated solutions for both the healthcare and logistics sectors.

# Problem 1: Damage to Reputation

Social media has grown into a world-wide battery, fueling every human with the ability to express their thoughts on various platforms about anything they would like. Because of this, businesses have a tremendous amount of weight on their shoulders to protect their image. “Reputational damage often results from a gap between what a company says and what it is perceived to have done.”[[3]](#footnote-4) Businesses must be careful in their handling of employees, stakeholders, and their customers because of the ever-growing social media presence in society. “According to Aon’s 2019 Global Risk Management Survey, damage to reputation or brand is the second top risk out of 15 risks,”[[4]](#footnote-5) this is a survey that was completed by decision-makers from 60 countries. The presence of entrepreneurs, their employees, and the business’s own social media accounts are seen, and customers take note of their professionalism.

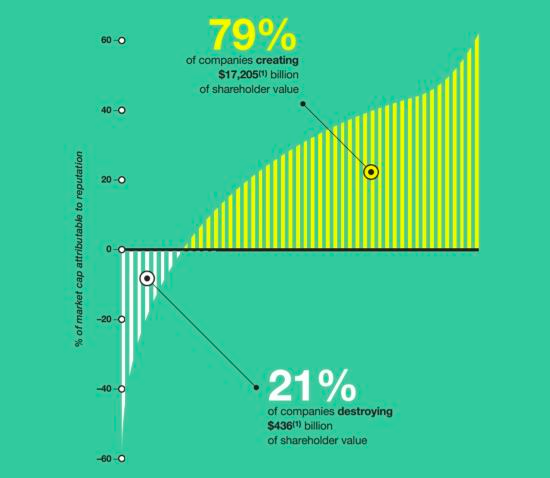
The result of reputational damage on a business has many impacts, ultimately adding up as a financial disaster. One result of reputation damage is fallen sales, as the public perception of the business is at a low point. Negative press is readily spread across social media, and the public can access reports about a mistake that was made by either the business or its employees. “According to a BrightLocal survey, 93% of consumers read online reviews.”[[5]](#footnote-6) As the number of potential consumers reading online reviews grows, businesses with bad online reputations are affected more because consumers will likely not use that businesses services. The quantified impact of losing customers is a tremendous impact for as long as the negative press lingers around the businesses brand. If 93% of consumers read online reviews (as said in the quote above) for this business, imagine the lack of sales and services that the business will be making – and the massive loss of revenue from it.

Another result of damaged reputation is lower retention of employees and potential hardships when it comes to recruiting new talent. There are a couple factors that contribute to this, fear of job security and appearance of poor leadership within the business. A 2016 Harvard Business Review survey reported that “a company with 10,000 employees could be spending as much as $7.6 million in additional wages to make up for poor reputation.”[[6]](#footnote-7) This is due to the pay increase requested in order to convince candidates to take jobs at such companies with poor public reputations. While it will take premium salary increases to hire new workers, it is also the case that many workers will leave the business or totally rule out applying for a job with that business in the first place. Say an employee’s messages about mistreatment in their job field are leaked and spread across news headlines and across media platforms. Many people seeking jobs in this field would instantly turn away from applying to work at this business. Unemployed workers, like consumers, use reputation when applying for jobs and finding which company they would like to work for.

On top of these, are the looming penalties and fines that will be given to the business because of their wrongdoings. No matter if the reputational damage is the because of the business or the employee, there will be fines for breach of compliance. For example, with HIPAA, healthcare businesses may face a maximum fine of $50,000 per violation depending on the tier of violation committed (HIPAA). One violation, for instance, could come from one singular post on social media. This is a serious threat to businesses, who must make sure those who work for the business promote only positive things about their workplace on social media. It is detrimental for businesses to face fines for violations; while on top of the one-time fine, companies will see the adverse result of bad reputations.

Along with various penalties handed to businesses by the government, lawsuits that may be brought about against a business can tarnish its name. Lawsuits and public litigation that involve businesses reveal unprofessional behavior that took place, often appearing in the media as it comes to light. Lawsuits drain finances and resources, and small businesses may not be able to operate after losing such lawsuits due to their low budgets. Another impact on businesses when it comes to lawsuits is relationships, as there may be severed ties as a result of misbehavior. “Publicized disputes can tarnish a company’s reputation… Litigation can ultimately decline a company’s value, drive down sales, or even cause a business to fold.”[[7]](#footnote-8)

Specifically, logistic companies face a few different challenges than those mentioned above when reputational damage is on the table. Healthcare companies fall under the same umbrella of financial penalties and lawsuits with such confidential information being involved. For logistic companies, however, there are many supporters behind the company that are stockholders and stakeholders that fund the business.



(Image: www.comprend.com)

Above is an image that was a result of a study done covering the largest companies in the world. “Of the 1,611 companies that were included in the study, 79% saw a positive effect on their reputation, while 21% actually saw a negative result.”[[8]](#footnote-9) This, however, is not the key result to be examined. The substantial percentage of businesses that increased their shareholder value created only $17+ billion, however, the small percentage destroyed $436 billion in value. This shows how detrimental negative light is to companies. When reputation is tarnished, the contributions of those who want a business to succeed are wasted, resulting in a downhill trajectory for the future of the business.

# Problem 2: Distribution of Confidential Information

While talking about the damage to an organization’s reputation resulting from social media use is extremely important, it’s not the only issue facing companies. Another issue social media can cause to organizations is the concern of the distribution of their confidential information. While information can be distributed intentionally, or unintentionally, it is important to delve into this privacy concern for all types of organizations. Social media platforms share information in many ways. Social media is a complex topic, and many platforms can share information without users being aware. Depending on the platform’s privacy agreement, some information is defaulted as publicly visible, and many platforms allow for their users to redistribute information posted by others. Social media platforms do not take full responsibility to ensure that your information is secure, so it is important for each organization to have social media policies and monitor it closely (Rachamalla).

Distribution of confidential information is when company information that should be kept private is distributed. Confidential information is defined as, “information disclosed to an individual employee or known to that employee as a consequence of the employee’s employment at a company.”[[9]](#footnote-10) It can be in many different forms, not just written information. In fact, a lot of companies keep confidential information electronically as technology has become such a driving force in business today. Confidential information can be classified as business plans, employee’s personal identifiable information, passwords, customer information, payroll, etc. (Schwegman Lundberg & Woessner). It can be used against companies in many negative ways if leaked to the public. Distribution of confidential information can lead to competing companies gaining a competitive advantage, exposing employees’ personal information, and even more ways.

Social media makes this issue a bigger threat because of how easy it is to spread information on platforms. Distribution of confidential information can be a threat to organizations because of employees. Employees should always be trained when first hired on the social media policy and how to handle company information. This training should also be reviewed overtime, to ensure employees follow guidelines and safe practices. Employees can sometimes feel the need to post information online about their job, to vent. If the information they post about an event online holds information that should have been kept private, that can result in termination and a leak in privacy. Especially for organizations like healthcare, it is important to keep patient stories and interactions off social media, in fear of breaching HIPAA. A direct example of how this can happen is given in a report titled ‘Social Media and the Workplace,’ “For example, consider a corporate attorney working on a merger and acquisition who updates her Facebook status to read: ‘So glad the deal is done. I need some sleep!’ Someone who knows that the attorney handles mergers and acquisitions and represents a particular client may piece together that something important is about to happen.”[[10]](#footnote-11) This could lead to an unwanted outcome in that case. Sensitive information can be mishandled so easily and is an extreme concern, especially for larger companies who have people searching for information online about their competitors. Employees are some of the biggest threats that an organization must control, which can be done with policy agreements, proper training, and education on expectations.

Another way confidential information can be distributed is through social engineering attacks. A social engineering attack is when an attacker tricks an individual into revealing confidential data. For example, an attacker could easily pose as another employee working in the company’s IT department and message an employee on social media asking them for their login credentials. While hopefully most employees would be trained to verify this, some could fall victim. There is also profile cloning, where an attacker can create a fake social media account posing as a fellow employee and reach out to a ‘coworker’ asking for data on something business related (Stone). Many people would easily fall victim to this, as they probably would not think to double check if there was more than one account under that specific name. Once the employee shares that confidential information, there is no going back, and they most likely will not realize they made a mistake until the information is already compromised. The attacker could then post any business data that the employee gave to them, resulting in distribution of confidential information.

One main threat regarding social media security and employees is social media phishing. Social media phishing is defined as, “an attack executed through platforms like Instagram, LinkedIn, Facebook, or Twitter. The purpose of such an attack is to steal personal data or gain control of your social media account (Trend Micro).”[[11]](#footnote-12) This can happen when an employee receives a malicious link from another employee on a social media platform. For example, a link could be sent on LinkedIn, which is a popular website for networking with other business professionals (Stone). Most people would not be on the lookout for malicious attacks on professional websites. There are tools that make phishing attacks easier to accomplish like Hidden Eye or ShellPhish. These tools can help retrieve a person’s password, personal information, and any confidential information they have on their account (TrendMicro). It can give the attacker access to their account, making it possible for them to post the confidential information directly from that employee's account. If the attacker has access to the employee’s account, for example their LinkedIn account, they could easily impersonate said employee and send phishing messages to other people in their network or business to get their information as well, making the company even more in danger to leaked confidential data (TrendMicro). In some attacks, users will be directed to a website once clicking on a link, and although it might look like Facebook, for example, it could be a fake website where the attacker collects their credentials and then can post information through their account (TrendMicro).

Privacy and security can be difficult goals to accomplish now that social media is so relevant in today’s personal and business environments. Privacy is important to a company because of what it represents. If a company is not able to keep confidential information private, it is likely that it will not be seen as a professional, well-kept company. Companies could lose employees, customers, business deals, etc. Especially since many companies choose to have a social media presence, it is more important than ever to implement safeguards and controls to protect against social media attacks. Different companies will likely handle these issues in different ways, specifically for their unique needs and wants, meaning every company needs to look at specific solutions that will protect their confidential data and reputation.

# Solution for Healthcare Companies

Healthcare is one such industry where the privacy and security of information can be at risk due to social media. Social media presents quite a few problems because of the creation of social media applications that allow the sharing of electronic health records. Keeping patient and healthcare employee information strictly confidential has become more of a challenge because of these applications. Information is becoming more widespread and accessible than ever before as the healthcare industry relies more and more on technology. Because of this, it is not always easy to safeguard patients’ information and operate efficiently, especially under HIPAA and the security rules the healthcare industry must follow.

HIPAA, which is also known as The Health Insurance Portability and Accountability Act, “is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge.”[[12]](#footnote-13) There are two rules that make up HIPAA: the privacy rule and the security rule (Choi). The privacy rule addresses the proper handling and disclosure of sensitive information by individuals who must comply with the rule. Its main goal is to ensure an individual’s information is protected properly while also allowing this health information to be used to “provide and promote high-quality healthcare, and to protect the public’s health and well-being.”12 The security rule addresses the protection of data from outside threats. It covers all healthcare information that is transmitted electronically but does not apply to information that is spread by word-of-mouth or information that is written. To comply with this rule, all entities who handle electronically protected health information (e-PHI) must ensure the confidentiality, integrity, and availability of e-PHI, detect and safeguard against potential threats, protect against the improper use of e-PHI, and certify compliance by their workforce (CDC). Under HIPAA and the two rules associated, people expect their personal health information to be safe and protected. Otherwise, they may be entitled to take legal action against a healthcare organization in the event of a data breach or other attack. This gives reason as to why information security is such an integral part of the healthcare industry.

Protecting the confidentiality of information has become more of an issue as many companies have opted to use electronic health records and as social media becomes more prevalent in everyday operations. These records make accessing medical information easy and convenient for patients and helps them share it with their provider and others such as family or friends (Abunadi).The automation of healthcare information also helps keep organizations competitive and frees up valuable time that can be spent elsewhere (Choi). However, with increased accessibility through mobile healthcare apps also comes the increased risks of privacy and security issues. Some of the main threats to electronic health records include social engineering, malicious code, executive impersonation, phishing, and impersonation (Al-Muhtadi).All these threats can put the confidentiality of electronic health records on the line which can lead to a violation of HIPAA should they occur. Furthermore, confidentiality is not the only thing at risk when it comes to attacks on organizations. The organization’s image can also be on the line. Maintaining a positive public image and a good reputation with clients and patients is essential to business operations. A tarnished reputation because of an attack can draw people away and damage established relations with other healthcare organizations.

Social media itself is not harmful to the healthcare industry. In fact, it can be used in many positive ways. Doctors can post information that other doctors can use to save more lives, patients can post about certain healthcare organizations urging others to go there should they need treatment, and the organizations can use social media to promote themselves in order to extend their reach in the surrounding community. Social media can be a viable tool for marketing, education, and treatment, but it can also intentionally or unintentionally violate legal and ethical standards in the healthcare industry (Showalter). Most instances where violations occur are entirely unintentional. For instance, a family member keeping other family updated on a patient’s condition on social media is okay. However, if a healthcare worker who is involved in the treatment of the patient posts the same thing, it violates HIPAA. The healthcare worker, even with nothing but good intentions in mind, intrudes on the privacy of the patient and releases their condition for the public to see (Showalter).

While there is no one solution to protecting all patient and employee medical records on social media, companies in the healthcare industry can implement plenty of measures, safeguards, or policies to comply with HIPAA and prevent the spread of information. Unfortunately, ensuring the security and privacy of health information is no easy task and it can be called nothing less than complex and time-consuming. The whole healthcare organization must work together from top to bottom with the active involvement of every member exposed to healthcare information (Choi). The best place to start, regarding complying with HIPAA on social media, is making all individuals involved aware of what it is, how it works, and why it’s important. These individuals should be encouraged to not take pictures, record information on their cellphone, gossip online, or use social media at all when working in order to ensure privacy. Likewise, healthcare organizations should implement strictly enforced policies, form interdisciplinary teams, and assign an individual the responsibility of managing social media policy in the workplace (Showalter).

Organizations have more control over the security and privacy of information when it comes to handling the behavior of their employees on social media. What they have less control over are the outside threats to health information. Healthcare organizations must invest in safeguards and controls to make this confidential information hard to reach and access without proper authorization. Some of these safeguards would include firewalls, VPNs, encryption, and multi-factor authentication. Though these are important and add additional layers of security, they can be expensive to implement, which is why there needs to be more of an emphasis on the proper management and training of employees. Outsiders to an organization will try to manipulate employees, threaten them, send phishing e-mails, or even impersonate a higher-up. If an adequate amount of training has been provided, an employee should not fall for these types of attacks and will not violate HIPAA by putting confidential healthcare information at risk.

# Solution for Logistic Companies

With the proliferation of social media platforms, it is no surprise that logistic companies are taking notice. In fact, social media is now an essential part of the marketing mix for many organizations. Social media can be used to promote brand awareness and connect with consumers on a personal level. However, social media can provide just as many negative effects as positive ones. On the one hand, it can be used to publicize a company’s products and raise awareness of important social issues. On the other hand, it can be used to spread misinformation and create negative publicity for a company. For a logistic company, keeping information confidential is vital to the organization's survival. However, there are ways to mitigate the risks of using social media platforms without compromising your integrity or putting your company at risk.

Many logistics companies continue to rely on the traditional business-to-business (B2B) marketing channels such as relationship management and cold calling. (Brandenburg). However, these channels are not as effective as they once were. Consumers have become increasingly skeptical of traditional marketing methods. Instead, they are turning to social media and online review sites to learn about new products and services to make better business decisions. With over 2 billion active Facebook users, 300 million active Twitter users, and 675 million LinkedIn users every month, social media has become one of the most important communication channels for businesses of all types (Turner). There are many benefits that come with using social media to promote your business, including increased brand recognition, connecting with clients, and reputation management. However, there are certain risks associated with using social media that you should be aware of before you get started.

One of the main risks associated with using social media is that it can lead to negative publicity for your company. Anyone who posts negative comments about your company on social media has the potential to tarnish your reputation among consumers and damage your brand image. An example of this happened in 2013, Burger King’s Twitter account was hacked, and the hacker made posts that contained racial slurs, obscenities, and references to drugs (Lutz). These types of attacks can easily spread through social media and lead to negative reviews and bad publicity for your company. To avoid this kind of situation, passwords should be changed regularly to reduce the risk of cyber-attacks and leaks of confidential information. Employees should also be trained on how to use social media professionally and properly to avoid any negative consequences for the business. In addition to the risk of negative publicity, there are other risks associated with using social media to promote your business.

Logistic companies must utilize many different kinds of software in order to keep track of warehouse inventory, any shipments, and other components of the supply chain. Logistic companies focus on settings on cloud applications, which can cause an issue if a certain setting is toggled off, allowing for an unauthorized attacker to access data (Cipher). Cipher is a tool logistic companies can use to apprehend data breaches and lower the risk of a loss of commission from hackers. Logistic companies oversee stakeholders' data and must handle that data in a secure manner. The use of controls can help that effort. Logistic companies have started using more operational technology. The use of this technology “opens new communications and wireless channels that are connected directly to T&L companies’ digital ecosystems.”[[13]](#footnote-14) This increases the risk of hackers gaining access to systems. The addition of tools like Cipher can help companies lower some of these threats, but it will cost a company to implement. Every company will need to perform risk assessments and determine if and how much money they want to spend to implement security measures for social media and cybersecurity in general.

BCG goes on to discuss how transportation and logistics companies are especially subject to cybersecurity attacks because of a lack of regulations and awareness. This can be combatted by cybersecurity policies, especially on social media dangers and how hackers can get access to information (BCG). The benefit of this step of the solution is that it is mostly free to companies. A company can have an experienced employee train other employees on why cyberattacks and the threat of social media is becoming increasingly important to logistic companies. The first step in attack chains is most commonly self-imposed threats. This is true because cyber-attacks usually result from the vulnerabilities in a company’s organizational processes and the ability of the employees that work there (BCG). Logistic companies should invest in Zero-Trust architectures by segmenting networks using demilitarized zone technology. This results in the attitude that everything trying to connect to a network should first be considered a threat. This is another solution that will cost a company money, but it is a needed tool. Another solution for the social media threats facing these companies is hiring more information security skilled individuals to deal with these issues. Since logistic companies only recently started using more technology, there is a lack of experienced cyber professionals. Another reason there is a lack is because many newly graduated cybersecurity students do not see logistic companies as an appealing workplace, one where they can be creative (BCG). There needs to be efforts in hiring and attracting more technologically skilled people, who can train employees on the dangers of social media and cyberattacks.

Social media platforms collect a massive amount of personal data that is vulnerable to hacking and data breaches (Epic). If your social media accounts are compromised, hackers can access personal information about your customers and use it to launch targeted phishing scams or identity theft schemes. This can result in a loss of revenue as damaged customer relationships lead to decreased sales and increased expenses by resolving the breach. Trust is essential in any supply chain, but the trust that exists can be exploited by hackers. A malicious actor could use a social media platform to gain access to sensitive supply chain data and disrupt operations to extort money and cause harm to the organization (Cipher). In order to mitigate the risk, companies must educate their employees about the importance of cyber security, implement appropriate security measures, and carefully vet any social media applications that they utilize. Keeping security and privacy measures an open and critical subject within the organization is the most effective way to prevent security issues that could compromise the integrity of supply chains.

# Conclusion

In conclusion, social media can be an excellent tool, but also a threat to organizations. The threats that social media poses, however, can be well-managed if proper resources are allocated to protecting everyone involved – customers, employees, and businesses. If this is fulfilled, social media can help businesses increase their customer platform, raise revenue, connect employees, and even more. When utilized with the correct safeguards in place, it is a great addition to a company. Every company is responsible for implementing controls unique to their needs, to protect the privacy and security of their systems, employees, and customers. Although it is important to implement these safeguards, it does not end there. It is essential that these safeguards continue to evolve as new threats also evolve – technology is consistently changing, and it is not possible to properly address privacy and security threats with outdated methods.

There are countless threats that can arise with social media, two of which were covered in detail: damage to reputation and distribution of confidential information. With worldwide access to social media, it is crucial that businesses can keep their name in a positive light in the public eye. With a tarnished reputation comes fallen sales, trouble with keeping (and hiring) employees, and harsh penalties and fines that must be paid. The distribution of confidential information is a serious threat to businesses and their advantage to grow and keep customers pleased. In some cases, such as the healthcare industry, keeping information confidential is essential and expected under certain rules and regulations like HIPAA. Failure to comply could lead to serious consequences for businesses so it is important to protect information from threats inside and outside the organization. In other organizations, like Logistics companies, the need results from earlier steps, like hiring more technologically savvy people and implementing policies. Employees are one of the greatest threats to confidential information being distributed, therefore the training and policies given to employees are integral to any company’s wellbeing. Employees can fall victim to many social engineering attacks, as well as malicious phishing attacks. Social media provides a plethora of avenues for these threats to be done more quickly and easily, which is a major threat to an organization's privacy. Although solutions were provided here for each type of company, every company needs to delve deep into their specific issues and implement the correct controls. Not every one company will need to same plan.

# Works Cited

Abunadi, Ibrahim, et al. “BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients.” Sensors (14248220), vol. 21, no. 8, Apr. 2021, p. 2865. EBSCOhost, <https://doi-org.echo.louisville.edu/10.3390/s21082865>.

Al-Muhtadi, Jalal, et al. “Cybersecurity and Privacy Issues for Socially Integrated Mobile Healthcare Applications Operating in a Multi-Cloud Environment.” Health Informatics Journal, vol. 25, no. 2, 2017, pp. 315–329., <https://doi.org/10.1177/1460458217706184>.

Brandenburger, Alaina. “6 Tips for Logistics Marketing to Help Customers Find Your Business.” Constant Contact, 27 Jan. 2021, [www.constantcontact.com/blog/logistics-marketing/](http://www.constantcontact.com/blog/logistics-marketing/)

Brooks, JoAnna. Social Media and the Workplace: Managing the Risks. 2010, <https://www.jacksonlewis.com/sites/default/files/docs/Social-Media-Workplace-Managing-Risks.pdf>.

Burgess, W. (2016, March 29). A bad reputation costs a company at least 10% more per hire. Harvard Business Review. Retrieved August 1, 2022, from <https://hbr.org/2016/03/a-bad-reputation-costs-company-at-least-10-more-per-hire>.

CDC. “Health Insurance Portability and Accountability Act of 1996 (HIPAA).” Centers for Disease Control and Prevention, Centers for Disease Control and Prevention, 27 June 2022, <https://www.cdc.gov/phlp/publications/topic/hipaa.html>.

Chan, S., Yehuda, E., Schaefer, R., Schneuwly, A., Zicherman, S., Deutscher, S., & Klier, O. (2022, May 9). Navigating rising cyber risks in transportation and Logistics. BCG Global. Retrieved August 7, 2022, from <https://www.bcg.com/publications/2021/navigating-rising-cyber-risks-in-transportation-and-logistics>

Choi, Young B., et al. “Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules.” Journal of Medical Systems, vol. 30, no. 1, Feb. 2006, pp. 57–64. EBSCOhost, <https://doi-org.echo.louisville.edu/10.1007/s10916-006-7405-0>.

“Cybersecurity for Logistics Companies.” Cipher, cipher.com/cybersecurity-for-logistics/. Accessed 7 Aug. 2022.

Dixon, S. Share of U.S. population who use social media 2008-2021. 27 July 2022. <https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/>.

Hanbury, Mary. Lululemon issues an apology after an employee promoted an offensive T-shirt on social media, provoking a backlash online. 21 April 2020. <https://www.businessinsider.in/retail/news/lululemon-issues-an-apology-after-an-employee-promoted-an-offensive-t-shirt-on-social-media-provoking-a-backlash-online/articleshow/75274587.cms>.

HIPAA Journal. (2022, July 18). What are the penalties for HIPAA violations? 2022 update. HIPAA Journal. Retrieved August 1, 2022, from <https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/>.

Kenton, Will. Social Engineering. 27 March 2022. <https://www.investopedia.com/terms/s/social-engineering.asp>.

Lutz, Ashley. “Burger King’s Twitter Got Hacked and Tweeted Crazy McDonald’s Messages.” Business Insider, 18 Feb. 2013.

McGregor-Wood, Simon. Facebook Details Force Israeli Military to Cancel Operation. 4 March 2010.

Molok, Nurul Nuha Abdul. "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats." Edith Cowan University Research. Victoria, 30 November 2010. Electronic Article.

N, D. (2019, December 12). Impact of lawsuits and litigation on Brand Image - Supply Wisdom. Supply Wisdom - Continuous Risk Intelligence. Retrieved August 1, 2022, from <https://www.supplywisdom.com/resources/impact-of-lawsuits-and-litigation-on-brand-image/>.

Patel Date, Dee. “The Dangers of Sharing Personal Information on Social Media.” Penn Today, 19 May 2020, <https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media>.

“Protecting & Handling Confidential Information.” Schwegman Lundberg & Woessner, 29 Aug. 2019, <https://www.slwip.com/resources/protecting-handling-confidential-information/>.

Rachamalla, Anil. “Importance of Social Media Security.” End Now Foundation, 10 May 2021, <https://www.endnowfoundation.org/importance-of-social-media-security/>.

Salazar, L. R. (2021, January 28). Be careful what you post: social media and reputation. ProfSpeak. Retrieved August 1, 2022, from <https://profspeak.com/be-careful-what-you-post-social-media-and-reputation/>.

Showalter, J. Stuart. “Unintended Consequences: Patient Privacy in the Age of Social Media.” Hfma, 2018, <https://www.hfma.org/topics/trends/58918.html#:~:text=Unintended%20Consequences%3A%20Patient%20Privacy%20in%20the%20Age%20of%20Social%20Media,-Summary&text=Although%20a%20valuable%20tool%20for,legal%20and%20ethical%20confidentiality%20standards>.

Sickler, J., & Rice, D. (2020, May 8). What does a bad business reputation cost? Home -. Retrieved August 1, 2022, from <https://www.commpro.biz/what-does-a-bad-business-reputation-cost/>.

“Social Media Privacy – EPIC – Electronic Privacy Information Center.” Epic.org, epic.org/issues/consumer-privacy/social-media-privacy/.

Staff, SC. Study: Phishing scams cost large US companies about $15 million a year. 17 August 2021. <https://www.scmagazine.com/news/phishing/study-phishing-scams-cost-large-us-companies-about-15-million-a-year>.

Stone, Mark. “Social Engineering and Social Media: How to Stop Oversharing.” Security Intelligence, 13 Jan. 2021, <https://securityintelligence.com/articles/social-engineering-and-social-media-oversharing/>.

Turner, Justin. “Using Social Media to Attract New Logistics & Supply Chain Clients.” Flock Freight, 13 Nov. 2017.

Unauthorized access accounts for 43% of all breaches globally. 8 June 2021. <https://www.helpnetsecurity.com/2021/06/08/unauthorized-access-breaches/>.

Wennergren, H. (2019, December 18). How your reputation impacts your shareholder value. Comprend. Retrieved August 1, 2022, from <https://www.comprend.com/insights/2019/how-your-reputation-impacts-your-shareholder-value/>.

What is Phishing? n.d. <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works>.

What is reputational damage? what are its effects? Alva. (2021, March 10). Retrieved August 1, 2022, from <https://www.alva-group.com/blog/what-is-reputational-damage/>.

“What Is Social Media Phishing?” Trend Micro, <https://www.trendmicro.com/en_us/what-is/phishing/social-media-phishing.html>.

Wire, Nexstar. 533 million Facebook users were hacked. Here's how to find out if you were one of them. 5 April 2021. <https://www.kxan.com/news/533-million-facebook-users-were-hacked-heres-how-to-find-out-if-you-were-one-of-them/#:~:text=(NEXSTAR)%20%E2%80%93%20More%20than%20533,32%20million%20in%20the%20U.S>.

1. Kenton, Will. “*Social Engineering*”. https://www.investopedia.com/terms/s/social-engineering.asp [↑](#footnote-ref-2)
2. “What is Phishing?”. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works [↑](#footnote-ref-3)
3. *What is reputational damage? what are its effects?* Alva. (2021, March 10). Retrieved August 1, 2022, from https://www.alva-group.com/blog/what-is-reputational-damage/ [↑](#footnote-ref-4)
4. Salazar, L. R. (2021, January 28). *Be careful what you post: social media and reputation*. ProfSpeak. Retrieved August 1, 2022, from https://profspeak.com/be-careful-what-you-post-social-media-and-reputation/ [↑](#footnote-ref-5)
5. Sickler, J., & Rice, D. (2020, May 8). *What does a bad business reputation cost?* Home -. Retrieved August 1, 2022, from https://www.commpro.biz/what-does-a-bad-business-reputation-cost/ [↑](#footnote-ref-6)
6. Burgess, W. (2016, March 29). *A bad reputation costs a company at least 10% more per hire*. Harvard Business Review. Retrieved August 1, 2022, from https://hbr.org/2016/03/a-bad-reputation-costs-company-at-least-10-more-per-hire [↑](#footnote-ref-7)
7. N, D. (2019, December 12). *Impact of lawsuits and litigation on Brand Image - Supply Wisdom*. Supply Wisdom - Continuous Risk Intelligence. Retrieved August 1, 2022, from https://www.supplywisdom.com/resources/impact-of-lawsuits-and-litigation-on-brand-image/ [↑](#footnote-ref-8)
8. Wennergren, H. (2019, December 18). *How your reputation impacts your shareholder value*. Comprend. Retrieved August 1, 2022, from https://www.comprend.com/insights/2019/how-your-reputation-impacts-your-shareholder-value/ [↑](#footnote-ref-9)
9. Protecting & Handling Confidential Information.” *Schwegman Lundberg & Woessner*, 29 Aug. 2019, https://www.slwip.com/resources/protecting-handling-confidential-information/. [↑](#footnote-ref-10)
10. Brooks, JoAnna. *Social Media and the Workplace: Managing the Risks*. 2010, https://www.jacksonlewis.com/sites/default/files/docs/Social-Media-Workplace-Managing-Risks.pdf. [↑](#footnote-ref-11)
11. “What Is Social Media Phishing?” *Trend Micro*, <https://www.trendmicro.com/en_us/what-is/phishing/social-media-phishing.html>. [↑](#footnote-ref-12)
12. CDC. “Health Insurance Portability and Accountability Act of 1996 (HIPAA).” Centers for Disease Control and Prevention, Centers for Disease Control and Prevention, 27 June 2022, <https://www.cdc.gov/phlp/publications/topic/hipaa.html>. [↑](#footnote-ref-13)
13. Chan, S., Yehuda, E., Schaefer, R., Schneuwly, A., Zicherman, S., Deutscher, S., & Klier, O. (2022, May 9). *Navigating rising cyber risks in transportation and Logistics*. BCG Global. Retrieved August 7, <https://www.bcg.com/publications/2021/navigating-rising-cyber-risks-in-transportation-and-logistics> [↑](#footnote-ref-14)