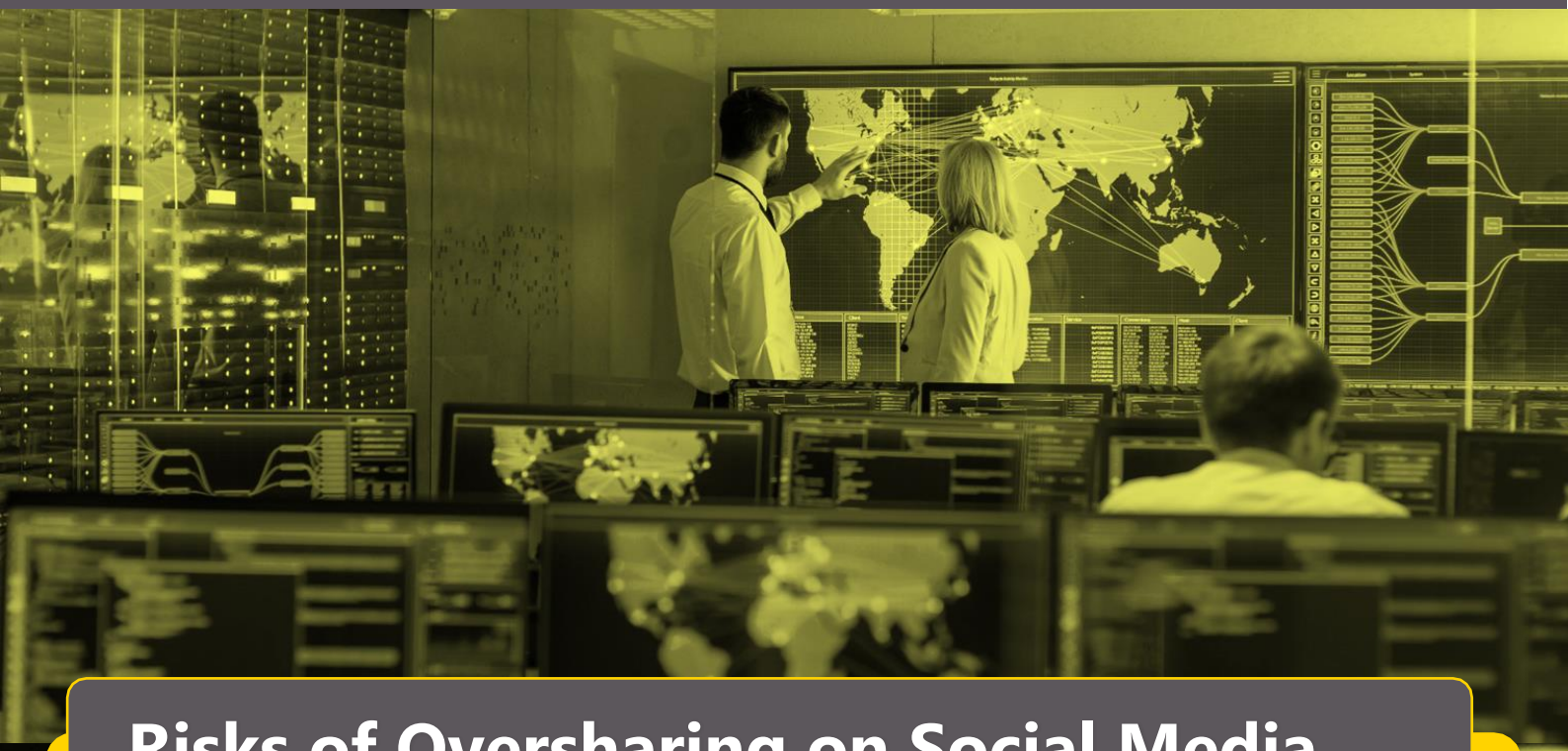
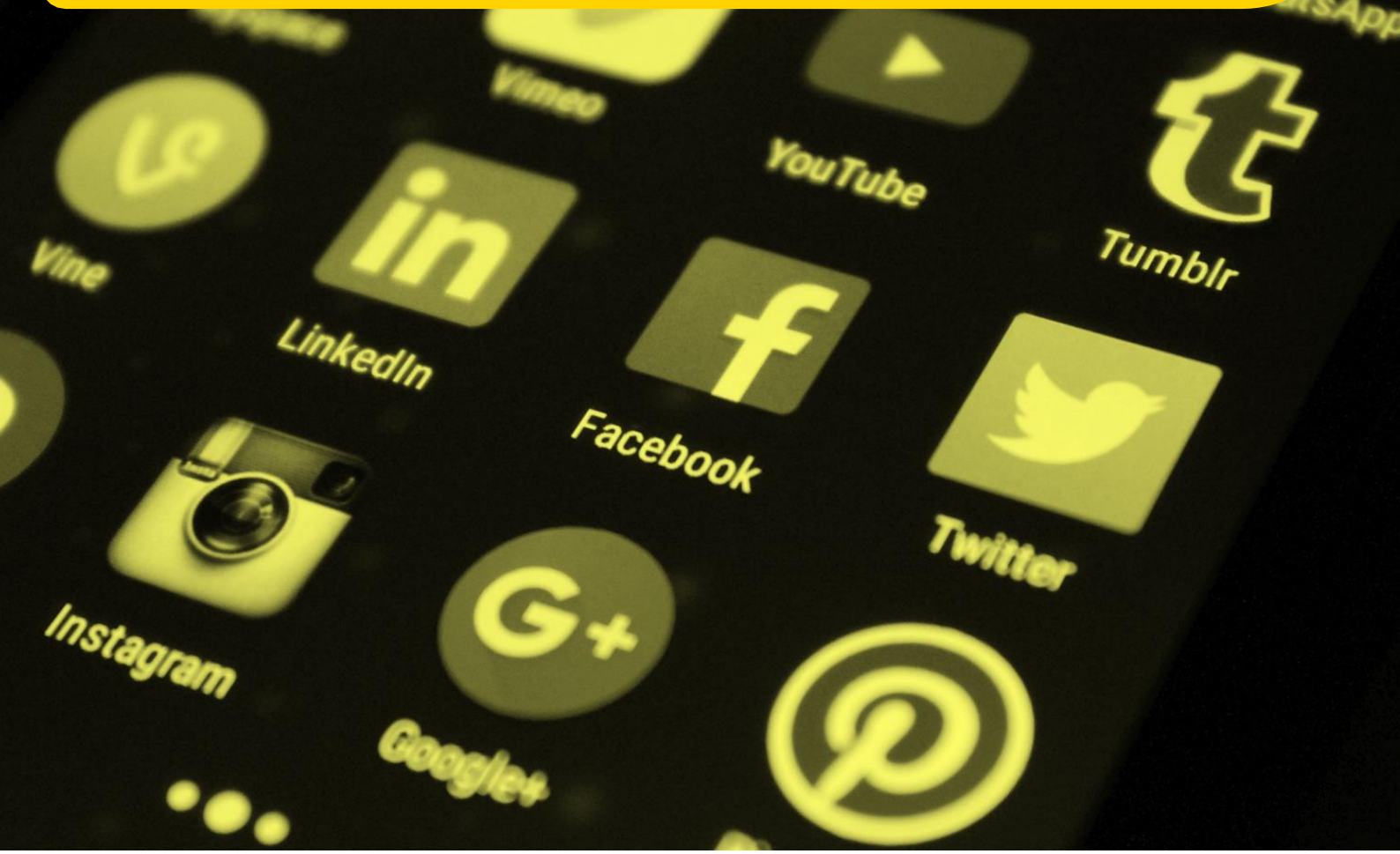
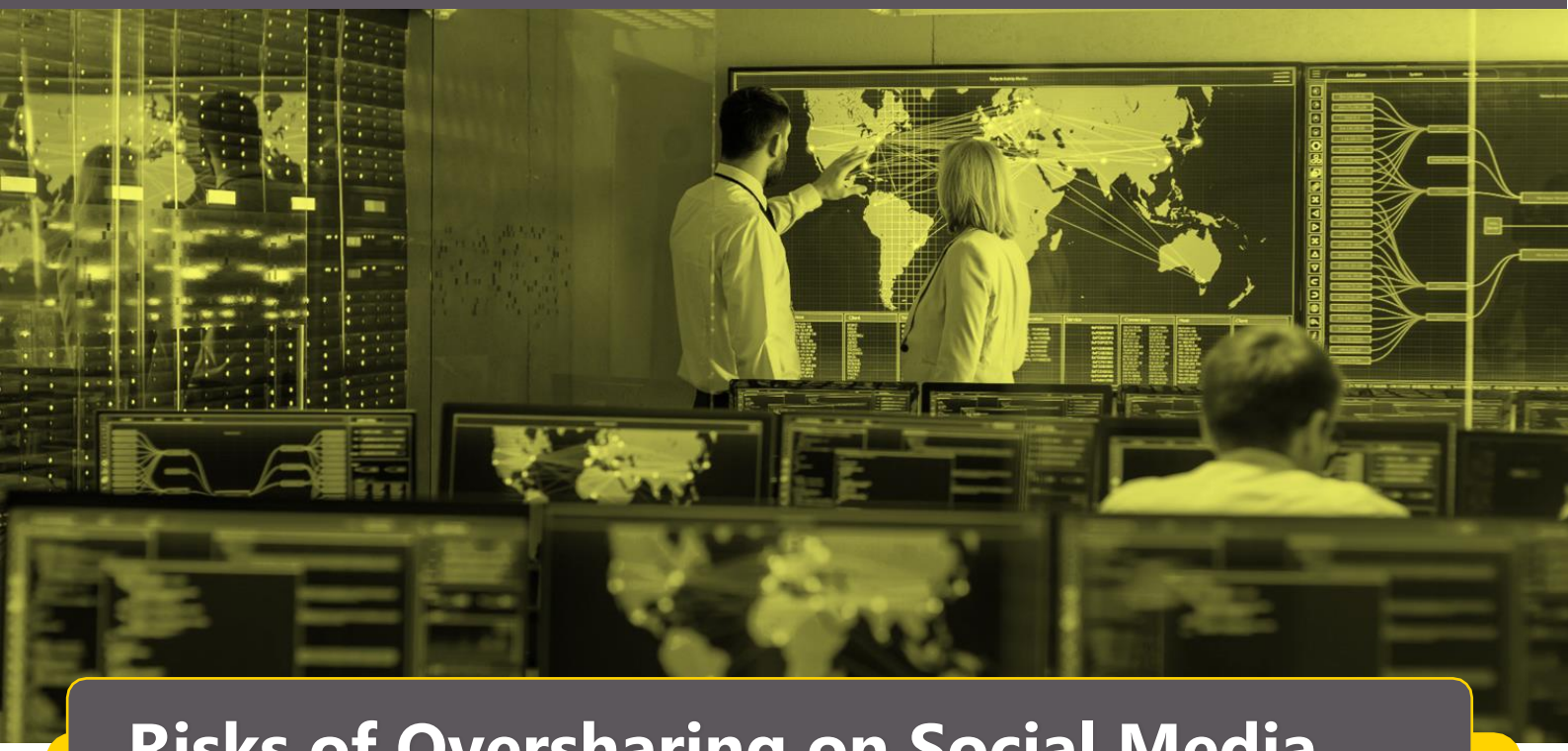


# Risks of Oversharing on Social Media

## Analysis of the LinkedIn Stories Feature





# Risks of Oversharing on Social Media

## Analysis of the LinkedIn Stories Feature

### Introduction

LinkedIn introduced a new feature to their platform this year called Stories. Although the feature was new to LinkedIn, the concept behind it is well known on other social media platforms. In 2011, Snapchat launched the first incarnation of the concept of temporary content being shared to friends. Snapchat focused on an adolescent audience, who did not want their private content to live online forever.

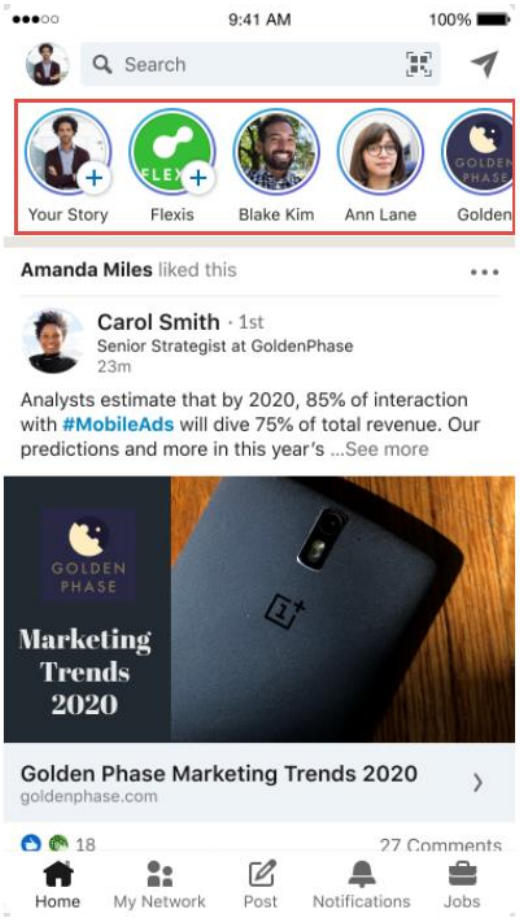
By the time this format reached other platforms like Facebook, WhatsApp, or Instagram, it was clear that the content shared did not always disappear. There are methods to save the posts in the story mode by simply taking a screenshot or video on the mobile device itself.

Finally, although the tool that LinkedIn is now launching follows an operation very similar to the one that made Snapchat famous, the target audience is not the same. The risks with this feature being used on LinkedIn are different. This document will cover more details about Stories and the risks of oversharing on this and other ephemeral platforms.

# LinkedIn Stories

## What are Stories?

Stories are a new feature that allows users to post photos and short ephemeral videos on your LinkedIn profile. The post is available 24 hours from publication. The content shared is treated differently from the rest of the content on LinkedIn. Stories appear in a row at the top of the main screen of the application only on the LinkedIn mobile app.




## What are they for?

According to a blog post written by LinkedIn's Director of Consumer Products Pete Davies, the company was looking for a lightweight way for members to interact in a professional context. In other words, the social network encourages the sharing of day-to-day videos and images at the office. This can be a privacy risk for the company.

## Who can see them?

First-degree contacts and followers will be able to view the story for a 24-hour period after it has been posted. In addition, your contacts can share it with anyone else on this social network through private messages. There is no privacy restriction that limits this action. Therefore, special care must be taken with all the information that you decide to share through this tool. Since any connection can see the posts, be careful with you connect with.

## Types of Risks and Recommendations

LinkedIn encourages users to connect with other members of their social network when there is some type of educational link or professional link. People often connect even if they do not personally know the person.

Therefore it is important for users to check their friends list and keep only the people they really know and trust. Otherwise, the person or the organization they are connected with represents may introduce risk: physical, reputational or technological. A cybercriminal can hide behind any type of identity on the Internet.


*Some users are already posting sensitive information with this tool.*

### Risks of Oversharing

The risk of data breaches and other cybersecurity damage often comes from insiders. Employees have easy access to computers, files and all kinds of confidential information. A misuse of the stories could lead to the leaking of not only the privacy of the person, but also of sensitive data of the organization itself.

In addition, the use of stories can make it easier to track people's locations. In recent days there have been cases of people who have published photographs, for example, of the plane tickets they use for business trips. In addition to the location and destination, the tracking of these documents allows obtaining personal data of the user that could lead to a risk of a social engineering attack.

In recent years, we are also seeing a greater presence of executives of large companies on social networks. This is usually part of specific communication actions of these companies that seek to show greater closeness with their potential customers. However, any publication that these types of profiles make at events or expos or in their day-to-day life, makes it easier to locate them. This is especially relevant through a tool such as stories that encourages the publication of content generated at a specific time.

## Risks to Reputation

In the case of using a company's branded account or a manager with significant media exposure, it is advisable to set some guidelines or establish a manager who defines the image you want to give and what content is published.

Using the new Stories feature may lead to spontaneous posting of posts with less restraint than usual. The publication of value judgments in these types of profiles or the exchange of comments in a high tone can damage not only the personal reputation of the executive, but also of the company itself.

Hence, only a series of authorized employees and knowledgeable about the company's strategy should be able to publish content. And this not only applies to stories, but to all social media accounts of the company or its executives.

Similarly, even the use of LinkedIn by employees in their personal profiles can harm the company's image. The way in which they represent themselves in this social network is still linked, even if implicitly, to their current and previous employers.

## Risks to Cybersecurity

Finally, there are a series of technological risks to using LinkedIn Stories. The risk is mostly derived from an incorrect use of this new LinkedIn function, which can compromise or expose personal data or user information:

- There is a risk of using third-party applications on mobile apps to make these videos more appealing. These applications could insert malware. For example, an application could be created that allows users to include virtual filters to improve the aesthetics of the publications made. When users install these applications, they often agree to the terms of use and privacy policies without carefully reviewing the details in the message, which may include granting permissions to the application.

- Risks of using unofficial browser extensions. Being a function available only in the mobile version, users could resort to downloading unofficial browser extensions (that is, not created by LinkedIn) in order to allow them to use the stories also in the web version. When installing this type of extensions, it is necessary to verify the app creator, since, as in the previous case, unofficial extensions could be malicious computer programs dedicated to stealing information.

- Risks of exposure of personal information: If a user shares through this function the activities they carry out on a daily basis, it is important to review with whom this information is shared. This is because cybercriminals take advantage of data they collect on social media to later scam and deceive their victims. A clear example, in this case, could be phishing. In addition to the information published on LinkedIn regarding the position or company where you work, the stories allow the cybercriminal to learn more personal details of the user: close co-workers, disposition of the job or even personality traits. This facilitates the use of social engineering techniques to build confidence in the victim and mislead them into taking improper actions, posing, for example, as a person from the company in an apparent official electronic communication.

- Risk of data leakage: When users post photos and videos, the files are stored on LinkedIn's servers. Therefore, cybercriminals who manage to breach the security barriers of this company could verify the code of the file to find the URL and download it.

## Conclusions

Using a professional network like LinkedIn is different than other networks like Facebook or Instagram. LinkedIn relies on people connecting with other professionals to create a network that adds value to our careers. Therefore, they do not necessarily have to be people with whom we have a personal relationship.

Hence, the idea that our publication through LinkedIn stories will disappear after 24 hours can give us a false idea of privacy. The information that we are publishing may reach a larger circle than we would like. In addition, if you include any type of personal information, this could be exposed and suppose a leak of information from our data or from the company in which we work.

LinkedIn allows your contacts to share your stories with anyone else on this social network through private messages. Furthermore, there is nothing you can do to avoid it. You just must be especially careful with the information you decide to share through this tool.

Managers of companies who are not used to social networks and who deal with information of special sensitivity should pay attention with this new function.

## Recommendations

The following are a series of recommendations for companies with an enterprise-level social media infrastructure to employ. Following these mitigates the risks associated with LinkedIn Stories or other ephemeral video features:

- Organizations should provide training on how employees should use social media, especially in their work environment. Social networks make it possible to determine who, within an organization, may be more susceptible to publishing confidential information through these tools. The damage could be done in an unintentional way.

- Master guides can be designed for the use of the corporate profile, as well as for those managers with significant media exposure. The appointment of a social media content manager who understands the company's strategy and the risks to which it is exposed for the organization and its employees can be valued.

- Many third-party applications request permission to access user data and information, as well as log in on behalf of the user. You should review with whom this information is shared and try to limit the use of these types of applications to what is strictly necessary.