Cesar - Unauthorized Use

Sources:

1. [https://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264](about:blank)
2. [https://ivypanda.com/essays/theft-of-information-and-unauthorized-computer-access-article/](about:blank)
3. [https://www.lexology.com/library/detail.aspx?g=208533ed-ecbe-4410-9fd9-f159f135884c](about:blank)

Unauthorized use or access refers to the access of a network, data, devices and other sensitive information without receiving permission. Authentication is set to verify a users identity but broken faulty authentication systems are the main cause of unauthorized use. Other common causes can be; weak passwords, social engineering attacks aiming to steal credentials, already compromised accounts that are linked to more secure systems. The first article source talks about computer technology in everyday existence, and how it's used to share and send personal and sensitive information. With this the most common threat in this is unauthorized access to this information, loss of confidentiality, information, etc. To reduce the damage, there are established systems to protect this information. The article discusses internal and external threats, and the ricks that can arise from this. As well as logical access controls, security policies and models, and logical access control mechanisms. The next article source talks about how information is important in successful organizations and how unauthorized use happens due to the organizations weak security strategies. Thus, making this sensitive information vulnerable. There can be loopholes in the security systems that others take advantage of in order to steal or corrupt an organization. This article brings up ways of unauthorized use that can be specifically related to a company. Giving examples on how it can happen because of disconnected employees, hackers, journalists and political activists and information agents. The last article source discusses the unauthorized use problem and the straight forward fix to it. It begins by detailing how many U.S. citizens receive emails about “credit card information being compromised”, this and other similar tactics are reasons to which security is breached. There is data given on how the percentage of unauthorized access is high to which it accounts for almost half of all security incidents. The author discusses how despite this high risk number, this can be avoided by; hardware disk encryption, firewall, antiviruses, back up and monitoring.