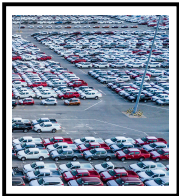


ISSUES OF THE DIGITAL AGE

CYBERATTACKS

Nowadays, fewer shoppers walk into stores and more interact with a digital interface. In a similar manner, we have completely forgotten cash and now use cards, but today our phones accompany a digital wallet. With technology so integrated into our daily lives, it's easy to take these aspects of our routine for granted. What we fail to realize is with one click, everything could be snatched out of our hands. Commonly referred to as cyberattacks.

Most recently, The United States saw a cyberattack on CDK Global this past week. CDK Global is known for making technology systems for car dealerships, handling marketing, customer relations and other tasks. As a result, CDK temporarily limited functions and car dealerships struggled to run their systems. Additionally, Bloomberg shares that the devastation faced by CDK global is now worth 1.2 trillion dollars.



Not only do such cyberattacks affect companies monetarily, but also highlight a growing gap in technical developments. Numerous professionals share that the complexity of such hacks are getting advanced day by day, making hackers stay undetected for longer. Adding to the issue is outdated software, entities using older platforms, such as government infrastructure become an easy target for hackers.

An FBI report found that healthcare, critical manufacturing and government facilities were targeted the most in cyberattacks. Forcing healthcare and other industries to find new alternatives. Hospital nurse from Rochester told CNN that healthcare workers are now resorting to paper charting. Creating a struggle between record keeping and patient health.

Attention is slowly being drawn to this issue, but not fast enough. According to a Cybersecurity Ventures report, in 2023 the cost of cybercrime hit \$8 trillion It is projected the total annual cost to rise to \$10.5 trillion by 2025.1



Numerous experts suggest companies implement data encryption to prevent personal and user data from being leaked. Additionally, frequent cyber security tests can be done to inform companies of the strength of their cybersecurity protection. Furthermore, incident response plans are highly essential for companies to professionally handle such situations.

Although the interaction between hackers and companies is increasing, as customers it's important to be on guard and prepared for technical delays. It might also be time to keep some cash on hand for when we can't shop online or use our digital wallet.

RESOURCES USED

<https://www.sangfor.com/blog/cybersecurity/cdk-global-outage-everything-you-need-know>

<https://www.autobodynews.com/news/cdk-global-cyberattack-has-downstream-effect-on-collision-repairers>

<https://www.reuters.com/technology/cybersecurity/blacksuit-hacker-behind-cdk-global-attack-hitting-us-car-dealers-2024-06-27/>

<https://www.cbtnews.com/cyberattacks-cripple-u-s-auto-dealerships/>

<https://www.cbsnews.com/news/cdk-cyber-attack-outage-auto-dealerships-cbs-news-explains/>

<https://www.cnn.com/2024/06/27/business/cdk-global-cyber-attack-update/index.html#:~:text=CDK%20Global%2C%20a%20software%20provider,on%20the%20auto%20sales%20industry.&text=Cyberattacks%20seem%20to%20be%20more,companies%20even%20longer%20to%20resolve.>

<https://www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics/>