Question: Find a recent news story regarding a data security incident and prepare a one to two-page report and discuss with the tutorial class.

Answer: **Cyber Security Incident faced by Zoom**

**Introduction**

With the rise of technology our world has completely changed. We are becoming more and more dependent on technologies each day. Also, COVID-19 has shut down all the educational institutes from colleges to schools, business world, software companies. While the entire planet is currently shutdown because of COVID-19 pandemic, most of the businesses and educational institutes have adapted work from home or learn from home policies that in turn has given rise to video conference technology ‘ZOOM’ in last few months. We all know that a technology can be a blessing as well as a boon. Though it served it purpose fully but ‘ZOOM’ has faced a cyber security challenge in April 2020.

ZOOM is an American communications technology company headquartered in California, for face-to-face communications and meetings. ZOOM userbase moved upward from 10 million in December to 200 million in March 2020, creating unexpected and potentially damaging cyber security challenges for the company.

**Background**

Zoom Video Communications started experiencing a service disruption as large number of users started using it during COVID-19 pandemic. This in turn started affecting meeting and calls of users all over the world. The issue wouldn‘t have worsen as at those time all schools were opening with virtual learning concept and employees around the world continued to work from home. This affected security and data privacy of the company, which caused some of the businesses and school systems to ban the use of Zoom.

There were more than 15,000 reports of problems with Zoom video. The zoom classified 76 percent of those problems as log-in issues. Zoombombings, where unwanted user entered the meeting and played bad.

**Response**

Reports by Sunday Times had revealed that the login details of over 5 lakh zoom users were found on the dark web where it was being sold for as cheap as 1 pence each which is even less than a rupee. As per the report, a company named Cyble which is a cybersecurity intelligence company bought the data from a Russian person through one of a messaging app Telegram.

ZOOM was soon made aware of this massive data breach, to which they issued an official statement, “We continue to investigate, are locking accounts we have found to be compromised, asking users to change their passwords to something more secure, and are looking at implementing additional technology solutions to bolster our efforts.” They also added, “It’s common for web services to be targeted by activity which involves bad actors testing large numbers of already compromised credentials from other platforms to see if they’ve been re-used.”

**Results**

Zoom took a 90-day security enhancement plan from April 1 to increase the security of the application. It also increased data privacy concerns for customers and built user trust, according to Zoom‘s CEO Eric Yuan. The 90 days ended on July 1. Zoom locked the hacked profiles and asked users to create a new one with strong password.

During those 3 months period, Zoom enacted a 90-day freeze on all features not related to privacy, safety, or security. The company said from April 1-July 1, it released more than 100 new security and privacy features, including Zoom 5.0, an updated platform that includes a support for AES 256-bit GCM encryption, a single icon that contains all security features, and the ability to report users for inappropriate conduct. Zoom is working on rolling out optional end-to-end encryption for all users, not just paid users, as of the end of July.

**Lessons**

This should serve as a power call to action for all companies to carefully consider privacy and security practices when engaging vendors and service providers, even now. Data security is of upmost priority, The rush to engage customers or users not only during COVID-19 pandemic should not be at the expense of privacy and security. We must try to keep our data safe.

When a company fails to protect our privacy, we shouldn’t just continue to use its product — and tell the people we care about to use it — just because it works well and is simple to use. Once we lose our privacy, we rarely get it back again.

**Conclusion**

In this era of technology, everything is data. Our life revolves around data. So it is a major concern when it comes to data security. No personal data should be shared with the other party without one’s consent. Thus data security plays an important role in any business, companies, third party, customers and users. All companies must take care of its partner as well as customers data.

**References**

* [**https://www.jdsupra.com/legalnews/zoom-lessons-learned-vendor-privacy-and-86864/**](https://www.jdsupra.com/legalnews/zoom-lessons-learned-vendor-privacy-and-86864/)
* [**https://en.wikipedia.org/wiki/Zoom\_Video\_Communications**](https://en.wikipedia.org/wiki/Zoom_Video_Communications)
* [**https://www.tomsguide.com/news/zoom-security-privacy-woes**](https://www.tomsguide.com/news/zoom-security-privacy-woes)