**Recent Security Breaches**

Student's Name

Institutional Affiliation

Course Number: Course Name

Professor's Name

Date

**Topical Security Breaches**

Most companies have shifted their daily business activities to paperless offices and moving to remote operations. The shift has caused a significant rise in data breaches, thus creating security concerns across the corporate world. According to Kaspersky Daily (2020), data breaches from cyber attackers use sophisticated hacking modules since the technological data storage models are ever-changing. The Kaspersky report shows that over 726 million attacks have been reported to occur since 2020 on the verge of Covid-19 attacks. The attacks have caused an average of 1.5 billion cyber-attacks annually. In the last two years, cybercriminals have exploited the Covid-19 uncertainty to initiate advanced data breaches to all potential industries (Kaspersky Daily, 2020). Data breach management continues to become a problem since most organizations are setting online platforms for data storage. The paper describes two data breaches across the USA and the U.K and possible containment measures for the data breach.

**BlueKai Data Breach on June 19, 2020**

BlueKai is a cloud-based large volume data platform that manages online and offline personalized data of various companies. BlueKai is owned by the U.S tech giant Oracle. BlueKai possesses extensive bank web tracking data that it stores outside the federal government intervention.  Whittaker (2020) notes that BlueKai's cloud-based data management platform uses cookies to follow users' activities on the web then sells the information to companies and marketing firms. However, the company faced malware intervention last year caused by a system malfunction. For an unknown time, the web tracking data from BlueKai was left exposed to a server that was not protected since it had no password. Billions of records were unsecured, and all attackers could find the data (Whittaker, 2020). The data breach was caused by human error, unlike others that occur because of social engineering errors.

The data breach leaked billions of records, including names, e-mails, home addresses, and identifiable data that includes user's web browsing activities. The data exposure made most companies use web users' information in their ads without the user's consent. Despite the core company Oracle saying they have managed the problem, the information has affected the advertisement sector. Bluekai data breach caused more uncertainties in the use of personal data in company's ads to show how some companies have high data consumption modules. BlueKai tracks and records approximately 1.2 percent of all Web traffic and has been following trends in websites like Amazon, Forbes, ESPN, and MSN.com (Whittaker, 2020). The amount of data left on the unsecured server created a blunder in the field of cybersecurity. The controversial effects of the data breach show that the company associates its leak with malpractices, as the website did not configure the causes of the data breach.

**Chartered Professional Accountants of Canada Data Breach, June 4, 2020**

The Chartered Professional Accountants of Canada (CPA) experienced data breaches and cyberattacks from March to June 2020. The data breach allowed unauthorized access of organizational information to gain access to the personal information of over 329,000 employees and stakeholders. According to Gatlan (2020), the stolen information had an impact on the organization since the attacker targeted personal information and information that related to managements strategies on the distribution of the CPA Canada magazine. The employees, members, and stakeholders lost personal data like names, e-mails, and general employer information. CPA Canada condemned the attack and assured members that irrespective of the attacker gaining access to passwords and credit card information, all the data from the two was protected and encrypted (Gatlan, 2020). All affected individuals by the breach had to be notified of the attack, and the organization considered effective security measures by notifying relevant authorities.

CPA Canada did accept the cyberattack and alerted members and contracted the law enforcement agencies for appropriate measures to curb the attack. All members and stakeholders were asked to ignore malicious e-mails and change their passwords on the CPA portal. According to Gatlan (2020), safeguarding organizational information was the most appropriate counteractive program aside from alerting members on the breach. CPA Canada was fast in mitigating worse effects by ensuring affected members do not fall victim to future phishing and malicious e-mails that target user's sensitive information like passwords. The data breach was discovered on an undisclosed date but was announced in June. CPA Canada continued to alter members on monitoring the security of the web platform and focusing on the integrity of their passwords to ensure the process remains secure from third parties intervention.

**Preventing Data Breach Incidents**

To prevent and monitor data breaches, all personnel in the organization need to monitor and ascertain their credibility since there might be malicious insiders. According to Chauhan & Kshetri (2021), the initial strategy could be remote controlling and monitoring. Around-the-clock remote control ensures I.T. personnel control and manage users' computers and alter the users on possible breach or malicious intervention. The other stage could be focusing on data backup and recovery since data breaches maliciously delete and encrypt organizational data. Organizations need to create servers that backup the data and cloud data that backup information in case of a server crash. For example, organizations need to set up automated remote backup systems that recover data on a regular basis in cases of loss or server crashes.

The affected organizations, BlueKai Company and CPA Canada by cyberattacks, need to set up patching modules and frequent software updates once all options are availed. Organizations need to focus on high-grade encryption to sensitize data. For example, all passwords and sensitive credit card information need to be encrypted so that third parties will not easily access the data. The update procedures should be related to data security standards to focus on consistent application of the set security measures. The strategies will ensure clear measures are taken and all employees work as per the security set measures that consider data as serious and sensitive (Chauhan & Kshetri, 2021). Additionally, BlueKai Company and CPA Canada organizations should focus on authorization to ensure data is handled by permitted personnel diplomatic personnel on data breaches.

The two organizations need to upgrade servers and all devices to ensure resilient software that is not easily breached. Once employees start working remotely, they can use personal devices for work activities, which can cause more controversies. BlueKai Company and CPA Canada need to enforce BYOD security policies. For example, all worker's devices need to use a VPN service and install the best antivirus software. Organizations all need to train and teach employees on the need for data protection. The last module is enforcing strong credentials and multi-factor user authentication since the aspect encourages effective cybersecurity practices.

**Conclusion**

Data breaches can be managed irrespective of cyber attackers using sophisticated hacking modules that are promoted by the rapid changes in the technological data storage models. The Kaspersky report also shows that over 726 million attacks have been reported to occur since 2020 on the verge of Covid-19 attacks. In the last two years, cybercriminals have exploited the Covid-19 uncertainty to initiate advanced data breaches to all potential industries. Data breach management continues to become a problem since most organizations are setting online platforms for data storage. The attacks have caused an average of 1.5 billion cyber-attacks annually.

**References**

Chauhan, P. S., & Kshetri, N. (2021). 2021 State of the Practice in Data Privacy and Security. Computer, 54(08), 125-132. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9504500>

Gatlan, S. (2020, June 4). CPA Canada discloses data breach affecting 329,000 individuals. <https://www.bleepingcomputer.com/news/security/cpa-canada-discloses-data-breach-affecting-329-000-individuals/>

Kaspersky Daily (2020). I T Security Economics 2020: Part 2. How businesses can minimize the cost of a data breach. Retrieved from <https://www.kaspersky.com/blog/it-security-economics-2020-part-2/>

Whittaker, Z. (2020). Oracle's BlueKai tracks you across the web. That data spilled online Billions of records were exposed. Retrieved from <https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/?guccounter=1>