**Seminar 5 – Preparation - Data Breach Case Study**

Read Swinhoe, D., 2020. The 15 Biggest Data Breaches of the 21St Century. [online] CSO Online.

*Select one of the cases by completing Data Breach choice. Once you have made your selection, you will be able to see the links to the case. Then complete a breach checklist as discussed in the lecturecast (reproduced below):*

*What types of data were affected?*

*What happened?*

*Who was responsible?*

*Were any escalation(s) stopped - how?*

*Was the Business Continuity Plan instigated?*

*Was the ICO notified?*

*Were affected individuals notified?*

*What were the social, legal and ethical implications of the decisions made?*

*If you had been the ISM for the organisation you selected what mitigations would you have put in place to stop any reoccurrences?*

**Case Study: Yahoo**

**What types of data were affected?**

Names, Email addresses, Telephone numbers, Encrypted or Unencrypted Security Questions and Answers, Dates of birth, and [Hashed](https://en.wikipedia.org/wiki/Key_derivation_function) [passwords](https://en.wikipedia.org/wiki/Password)

According to BBC news 23 SEP 2016 Yahoo says "state-sponsored" hackers stole data on about 500 million users in what could be the largest publicly disclosed cyber-breach in history. The breach included swathes of personal information, including names and emails, as well as “unencrypted security questions and answers”. The hack took place in 2014 but has only now been made public. In the UK it is believed data on about eight million user accounts was taken in the hack (Lee 2016).

**What happened?**

Attack Vector (how they got in): Improper Input validation allowed attackers to take on any identity they choose by exploiting a weakness in the creation of user identifying and authorizing cookies. Cookies are pieces of information that get stored on the client device to overcome the inherent stateless behavior of web servers. Because a stateless web server has no direct means to remember the state or connection details about a connected client, an identifying piece of information is stored on the client (think unique ID code) in the form of a cookie. This cookie should be unique for every user or client connecting to the server, and it will allow the web application to correlate details about the user, typically stored in a database, to the client connection. This allows a normally stateless connection to remember you logged in and use that login to tie your user account to a set of authorized actions. Imagine that if the information stored in a cookie, the information that uniquely identifies a user of the system isn’t that unique, can be stolen or is guessable (as was the case with Yahoo), now an attacker can assume the identity of anyone and use the privileges that come with that account to do evil. With 6 Modern Cybersecurity Practices that kind of access, an attacker can assume the identity of every user and individually download all their personal information or find a privileged user with access to the application’s database or other supporting systems to place themselves into a position where they can mass extract data or mass destroy resources. Identifiable information should be unique and impossible to guess and should be useless if somehow stolen. As per The Guardian, the hackers used “forged cookies” – bits of code that stay in the user’s browser cache so that a website doesn’t require a login with every visit, wrote Yahoo’s chief information security officer, Bob Lord. The cookies ́could allow an intruder to access users’ accounts without a password” by misidentifying anyone using them as the owner of an email account (Bpbonline 2020).

**Who was responsible?**

Bob Lord, Yahoo’s chief information security officer, said in a statement that the state-sponsored actor in the 2014 attack had stolen Yahoo’s proprietary source code. Outside forensics experts working with Yahoo believe that the state-sponsored hackers used Yahoo’s code to access user accounts without their passwords by creating forged “cookies,” short bits of text that a website can store on a user’s machine. By forging these cookies, attackers were able to impersonate valid users, gaining information and performing actions on behalf of their victims. The company has not disclosed who it believes was behind the attack (Goel & Perlroth 2016).

**Were any escalation(s) stopped - how?**

Yes, and here below are the steps taken from yahoo to stop (Matthews 2019).

* Invalidated unencrypted security questions and answers
* Continually enhancing the systems that detect and prevent unauthorized access
* Required all affected and unaffected users to change their passwords

**Was the Business Continuity Plan instigated?**

The data breach did not bring down the network. The immediate response to the security breach was to bring in security experts and consultants to conduct an investigation.

**Was the ICO notified?**

Yes, and Yahoo has been fined £250,000 over a hack from 2014 that affected more than 515,000 UK email accounts co-branded with Sky, the Information Commissioner’s Office has announced (Gibbs 2018).

**Were affected** **individuals notified?**

Yahoo and other news agencies release public notification, not to individually.

**What were the social, legal and ethical implications of the decisions made?**

Yahoo has been fined £250,000 over a hack from 2014 that affected more than 515,000 UK email accounts co-branded with Sky, the Information Commissioner’s Office has announced (Gibbs 2018).

**If you had been the ISM for the organisation you selected, what mitigations would you have put in place to stop any reoccurrences?**

-limit access to your most valuable data to employees.

-Third-party vendors must comply.

-Conduct employee security awareness training.

-Update software regularly

-Develop a cyber breach response plan

-Password security awareness to user.

-Implement latest security algorithms.

**References:**

Bpbonline (2020). *Yahoo Data Breach: What Actually Happened? – BPB Online*. [online] bpbonline.com. Available at: <https://bpbonline.com/blogs/news/yahoo-data-breach-what-actually-happened>.

Gibbs, S. (2018). *Yahoo fined £250,000 for hack that impacted 515,000 UK accounts*. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2018/jun/12/yahoo-fined-hack-ico-uk-accounts-russia>.

Goel, V. and Perlroth, N. (2016). Yahoo Says 1 Billion User Accounts Were Hacked. *The New York Times*. [online] 14 Dec. Available at: <https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html>.

Lee, D. (2016). Yahoo ‘state’ hackers stole data from 500 million users. *BBC News*. [online] 23 Sep. Available at: <https://www.bbc.com/news/world-us-canada-37447016>.

Matthews, K. (2019). *Incident Of The Week: Multiple Yahoo Data Breaches Across 4 Years Result in a $117.5 Million Settlement*. [online] Cyber Security Hub. Available at: <https://www.cshub.com/attacks/articles/incident-of-the-week-multiple-yahoo-data-breaches-across-4-years-result-in-a-1175-million-settlement>.