Seminar 5: Data Breach Case Study

The data breach case study concerns the Republicans National Committed data breach of data relating to 198 million American voters (https://www.upguard.com/breaches/the-rnc-files) containing information from the 2008, 2012 and 2016 American presidential campaigns.

Q: What types of data were affected?

The type of data breached in this case study, involved voter registration data of 198 million voters. 1.1 terabytes of unprotected data were breached which included birth dates, phone numbers, ethnicity, and religious views as well as data from Reddit posts and voter registration data. Roughly 9.5 billion data points of three out of every five American voters were scored on their likely political preferences modelled across forty-eight different categories.

Among the files publicly available for download, were indications of the repository's political importance with directories named for several high-powered and influential Republican political organizations.

Q: What happened?

The data was made publicly available on Amazon servers after Deep Root Analytics updated security settings.

Spreadsheets containing the breached data was exposed in a misconfigured database. The misconfiguration went unknown for an unknown period. On June 12th, UpGuard's Cyber Risk Analyst, on behalf of Cyber Risk Team, searched for misconfigured data sources. They then discovered an open an Amazon Web Services S3 bucket. The data repository lacked any access protection allowing anyone with an internet connection to access the data operation by navigating to a six-character Amazon subdomain, "dra-dw" (which stands for "Deep Root Analytics Data Warehouse").

Q: Who was responsible?

Deep Root Analytics confirmed they owned and operated the dra-dw bucket. However, the data was gathered and managed by Data Trust, a Washington-based firm created by the Republican National Committee to manage the GOP's voter file. Also involved were TargetPoint Consulting (acting as principal contact) and Causeway Solutions.

Q: Were any escalation(s) stopped? If so, how?

Shortly after they the federal authorities were notified, Deep Root Analytics secured the data against public access two days later, on June 14th.

Q: Was the Business Continuity Plan instigated?

Unknown.

Q: Was the ICO notified?

Yes, UpGuard's Cyber Risk Analyst notified the authorities, and the Data Analytics secured the data two days later.

Q: Were affected individuals notified?

No. In the case study, there is no mention that the voters were notified of the data breach. However, I make strong assumption that a notification was publicly available on the

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

The social implications of this data breach are an undermined trust in the electoral process. It calls into question the responsibilities owed to citizens—targeted by high-powered data analytics operations—by private corporations and political campaigns. Distrust in information systems is raised given their increased cyber risk surface. The cyber-attack surface is problematic because more information about citizens is being hosted in digital information systems.

What mitigations would you have put in place to stop any recurrences

1. The data must be stored securely.
2. Correct access controls must be assigned to the data and to those users who can manipulate it.
3. Regular penetration testing must be performed against the data endpoints to identify any new cloud database weaknesses.
4. After any software update, the system must be tested for access control.

Other Considerations

- Despite the Cyber Risk Analyst identifying the data breach, why did they attempt to download the 1.1 terabytes of data? I think that UpGuard's Analyst had no right downloading data despite being the individual who identified the breach.
- Rather distasteful from the breached data is the idea that the Republican National Committee modelled a person's race and religious views based on their own data, thus disregarding how the people identify themselves.

References