Georgia Tech: A Discussion on Data Breaches

The institute issued a breach notification which can be found here.

This work presents the data breach which took place at Georgia Institute of Technology and exposed around 1.3 million records. An unknown bad actor gained access to the Central Georgia Tech Database which was connected to a web application and cause a security failure. The authorities learned about the illegal access around March end and took immediate steps to correct the impacted application.

The breach included the records of staff and student applicants, current and former students and faculty along with records of alumni. It has been expected that the stolen information might include birthdates, names, social security numbers, and addresses. While the enrolment count of the faculty and students is around 27000, the magnitude of breached records suggests that the database contained historical data of alumni. It can be debated why would an institution store social security number of its alumni, students, and faculty especially when such information can have a long term negative impact on the privacy of individuals.

Even though the University System Georgia and US Department of Education have been notified and a thorough investigation is underway, the breach took place a year after a staff member had mass emailed confidential student data in July 2018. This highlights the weak security system which is prevalent within the institution. It can be argued how strong is the encryption of the institution's central database system. A simple investigation must start with the architecture of the institute's database management system. For example, how strong is a department database connected to the central database? Rather, how strongly will the central database impact if a department database is breached?

It is important to realize that even though security compliances follow strong guidelines or are strictly audited, there will be risks. Hence, time to time risk mitigation process must be in place through round-the-clock system improvements. Interestingly, the institute learned about the security failure after their developers detected significant impact in their performance around March end. This means the breach could have happened much before the institution actually realized while an official statement was released in the first week of April. Surprisingly, all these events suggest negligence of the authorities.

Such a breach is dangerous as:

- Education institutes are under constant attacks
- Privacy of faculty and students are under threat
- Historical data can contain sensitive information

While most investigate the failure and design a breach-proof methodology, less importance is given to the information which is stolen. Most stolen data are either exposed on the internet or proliferated to the dark web. It is worrisome because criminals can use information like credit card numbers, phone numbers, addresses, etc to cause harm. During a financial fraud, individuals are alerted and immediate steps are taken i.e. change of credit cards, portability of phone numbers. In other instances, when hacked, emails and passwords can be changed. However, unchangeable data like biometric information, social security numbers, and names, can pose as long-term threats to individuals if fallen into wrong hands. It can be in years!

Institutes can reduce the privacy threats of individuals in such cases if they avoid storing sensitive data and delete unnecessary information after a specific time interval.