Introduction:

Texas Department of Transportation Data Breach. This breach was discovered May of 2025, though it wasn’t publicly disclosed until the end of June 2025. This breach made headlines due to targeting a major government entity & the compromised personal information for over 1.8 million individuals in \* out of the state of Texas.

Describe the Breach:

TxDOT experienced a third-party supply chain data breach, not from a direct hack but through a vulnerability in Turnitin, its plagiarism detection vendor. Attackers exploited Turnitin’s systems to access data TxDOT had uploaded, making the agency an indirect victim. State agencies like TxDOT are attractive targets due to the large amounts of sensitive citizen data they hold, and threat actors often exploit weaker third-party vendors as back doors into these more valuable systems.

Identify the Threats:

I realized the gravity of the breach when I learned that 1.8 million names, social security numbers, birth dates, driver’s license details, and even addresses had been stolen. It struck me how easily criminals could turn this personal information into financial accounts, loans, or even fraudulent tax returns in someone else’s name. With such detailed data, they could also create convincing phishing attempts that many might fall for. What is most concerning is that this won’t end quickly. Information could circulate on the dark web for years, fueling long-term fraud. Beyond the immediate risks, we can’t ignore the deeper consequences: each new breach chips away at the public’s trust in government systems, and if third-party vulnerabilities remain unresolved, we could see the same scenario repeat across other agencies.

What could have been done to prevent this breach?

Strong security depends on a combination of technical safeguards and formal policies. Secure coding practices, such as rigorous input validation and sanitization, help prevent common vulnerabilities like *SQL injection*, while data encryption in transit & at rest ensures that stolen information remains unreadable without proper keys. Strict access controls, guided by the *Principle of Least Privilege*, further limit exposure by granting users and systems only the access they truly need. To reinforce these measures, organizations should adopt a *Third-Party Risk Management* policy requiring vendor security assessments and ongoing monitoring, a data classification and handling policy that defines sensitive information and dictates how it must be protected.

Final Summary:

The TxDOT breach is a strong reminder of how weaknesses in supply chain security can cause serious damage and why a layered, principles-based approach to cybersecurity is necessary. Following best practices like data minimization and thorough third-party risk management could have reduced the impact by limiting the data shared and spotting vendor vulnerabilities sooner. Triple A (AAA) principles also highlight what went wrong: stronger authentication with multi-factor methods might have blocked attackers using stolen credentials, authorization controls could have limited access even after the vendor was compromised, and better accounting through logging and monitoring might have detected unusual activity early enough to reduce the loss.

This incident also shows why relying on a single defense is not enough. A proper defense-in-depth strategy would combine protections at multiple levels: firewalls and segmentation for networks, secure coding and testing for applications, encryption for sensitive data, and strict policies and contracts for third-party handling. The breach happened because the vendor’s defenses at the application and data layers were weak, leaving TxDOT’s data exposed. To prevent future supply chain attacks, organizations must adopt true defense-in-depth, supported by AAA principles, to strengthen resilience and maintain public trust.

*Relations, M. (2025, June 6). Account compromise leads to Crash Records Data Breach. Texas Department of Transportation. https://www.txdot.gov/about/newsroom/statewide/account-compromise-leads-to-crash-records-data-breach.html*

*Malcolm, T. (2025, July 7). TxDOT Data Breach in May released 300K Crash reports. GovTech. https://www.govtech.com/security/txdot-data-breach-in-may-released-300k-crash-reports*

*TxDOT data breach 2025: 300K Crash Records exposed - what you need to know*. IDStrong. (2025, June 17). https://www.idstrong.com/sentinel/txdot-data-breach/