



Mar 04, 2019

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

[Robert W. Dibert](#)

Data Privacy Detective Podcast

Episode 31 – Data Incidents and Breaches: What mid-sized companies do when one hits

Data incidents arise regularly for businesses. The perpetrators range from sophisticated scoundrels seeking a quick ransom payment, to foreign governments conducting industrial espionage, to thieves seeking inside information, to distant hackers seeking personal data to sell on the dark web. When an incident arises, companies turn to legal counsel as part of the response team. In this podcast, [Bob Dibert](#), a Frost Brown Todd attorney with 30 years' experience and a veteran of data incidents, discusses how incidents arise and how they're handled.

There's a three-step approach when an incident arises.

- *Contain*: Immediately aim to stop further leakage and prevent additional harm from arising.
- *Counsel and Plan*: Promptly analyze the scope and nature of the incident, what needs to be done to address it both immediately and longer term.
- *Remediate*: Solve the problems, remedy the damage, notify those affected if required.

Not all incidents become data breaches. Data breaches refer to incidents where personal data has been compromised and notification to consumers or employees is required.

The average cost of data breaches and data incidents for mid-sized companies is not accurately known. Some surveys project an average cost of \$1 million, while others project an average data incident cost of \$5,000 to \$100,000, with a median of \$35,000.

Incident response needs to be immediate, so that incident response plans are best developed in advance, with a team ready to address a serious incident at a moment's notice. Because data breach

notification under GDPR and other regulatory regimes in the U.S. and elsewhere can require notice to data subjects within 72 hours, the response to data incidents should be rehearsed and available before one occurs.

Mr. Dibert shares a major lesson learned from years of experience with data incidents and breaches – educate everyone in a company to be vigilant about prevention. Anyone in a business can fall victim to a phishing or ransomware attack. Training and prevention are worth it.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.