BrittonTuma
business attorneys

digital business risk
infolert

Data Breach: Who's Gonna Get It?

The message–that's what I'm talking about–who's gonna get the message sent to them first?

Data breaches, hacking, and privacy are one of the biggest news stories since 2011 and there is no sign that will be changing anytime soon. By now even the most zoned-out among us should have heard of the hacking that led to data breaches by businesses like Sony, Citigroup, and Lockheed Martin. The list of companies that have been hacked seems like the Who's Who of the business world. Some reports even estimate that 90% of businesses have been hit by security breaches.

This is a big issue. Very big.

And you would think that business leaders would understand that their businesses could also be at risk for such a data breach and, if it were to happen, expose the business to significant liability under various data breach notification and privacy laws in many states. The hacking and data breaches are still happening, however. People's personal information is still getting exposed and nothing seems to be slowing down the hackers.

Why? Can they not stop this?

Is it impossible for businesses to prevent these data breaches? Is it perceived as being too expensive? Too troublesome to bother with? Is it really? How about I tell you a story that may demonstrate why it is definitely worth the trouble?

Have you ever heard of the Ford Pinto? The car itself isn't nearly as important as what it stands for in legal history: **big punitive damages awarded by an angry jury.**

The Pinto was an economy car that Ford built back in the 1970s that had one major problem: It exploded on impact. The structural design of the Pinto allowed the fuel tank filler neck to break off and the fuel tank to be punctured in rear end collisions which would occasionally cause deadly explosions. The even bigger problem according to the "Ford Pinto Memo" was that Ford knew it. Because it would cost $11 per vehicle to redesign Ford used a cost benefit analysis to determine that it would cost less to defend against wrongful death lawsuits stemming from such explosions of the car and consciously chose not to fix it.

In the case *Grimshaw v. Ford Motor Co.*, Ford was sued over such a death and the jury, learning of Ford's callous disregard for human life through this cost-benefit analysis, sent one heck of a message to Ford. **It awarded the plaintiff $2.5 million in actual damages and $125 million in punitive damages.** That's a lot of money (especially in 1970s dollars). Even though the punitive damages award was substantially reduced by the courts, it serves as a very good example of what juries can do when they get the feeling that big companies knowingly sacrifice the rights of individuals to save a couple of bucks.

What really impacted the jury was the fact that Ford knew the risks but consciously chose to do nothing about it because of what it would cost. Obviously the magnitude of loss of life is far greater than the loss of privacy so the situations are different in that regard. I can't help but think, however, that since the risks to breach of people's privacy rights are so well known now, companies that do not take adequate steps to protect those privacy rights are running a risk of being sent the same message that Ford got — especially if it is discovered that they could have prevented it but didn't to save a couple of bucks.

So the question is, "who's gonna get sent that message first?" Surely not your company, right?

If you have any questions about data breaches, breach notification, privacy or data security, please feel free to contact me to discuss.

Shawn E. Tuma
direct: 469.635.1335
stuma@brittontuma.com