# Privacy at the Heart of Colossal Cybersecurity Mistakes

**11.18.14**

Infoworld reported that for Information Technolgoy (IT) "Privacy has become one of the leading computer security issues today…Today's systems track every access, and every employee should know that accessing a single record they don't have a legitimate need to view is likely to be noticed and acted on." The November 17, 2014 Infoworld article entitled "10 security mistakes that will get you fired" includes these highlighted privacy mistakes by IT:

*Colossal security mistake No. 1: Killing critical business functionality*

*Colossal security mistake No. 2: Killing the CEO's access to anything*

*Colossal security mistake No. 3: Ignoring a critical security event*

**Colossal security mistake No. 4: Reading confidential data**

**Colossal security mistake No. 5: Invading privacy**

**Colossal security mistake No. 6: Using real data in test systems**

*Colossal security mistake No. 7: Using a corporate password on the Web at large*

*Colossal security mistake No. 8: Opening big "ANY ANY" holes*

*Colossal security mistake No. 9: Not changing passwords*

*Colossal security mistake No. 10: Treating every vulnerability like "the big one"*

The report included the following example of Colossal security mistake No. 5: Invading privacy:

*A friend worked at a hospital and once heard that a famous celebrity had checked in. The friend performed a quick SQL query and learned that the celebrity was in-house. They didn't tell anyone or do anything.*

*A few days later someone in the primary care staff leaked to a popular media site that the celebrity was being treated in the hospital. Management asked for an audit of who accessed the celebrity's records. The request came to my friend, who reported the results of the audit and self-reported their SQL query, though it had not been tracked by the information system. Management fired everyone who accessed the medical record without a legitimate reason. My friend, who would never have been caught if not for their aboveboard honesty, was fired without remorse.*

Other important privacy mistakes were reported with with Colossal security mistake No. 6: Using real data in test systems:

*When testing or implementing new systems, mounds of trial data must be created or accumulated. One of the simplest ways to do this is to copy a subset of real data to the test system. Millions of application teams have done this for generations. These days, however, using real data in test systems can get you in serious trouble, especially if you forget that the same privacy rules apply.*

*In today's new privacy world, you should always create bogus test data to be used in your test systems. After all, test systems are rarely as well protected as production systems, and testers do not treat the data in test systems with the same mentality as they do data in production systems. In test systems, passwords are short, often shared, or not used at all. Application access control is often wide open or at least overly permissive. Test systems are rarely secure. It's a fact that hackers love to exploit.*

Most people do not realize how vulnerable their privacy is within IT systems, and this report reminds everyone that cybersecurity mistakes expose us all.