Technical Update

How Secure is your Data?

Twitter, Target, and Yahoo are a few of the companies that have experienced data breaches that left their customers vulnerable to identity theft, brought on FCC investigations, and exposed the companies to litigation. Personal data has increasingly become a target of hackers. Taking the necessary steps to protect personal data protects you from the public relations and legal consequences of a data breach.

Strategies to Protect your Data

Do not collect unnecessary information. If you do not have the information in the first place it cannot be stolen. In a complaint against RockYou, a mobile gaming site, the FCC alleged that the company unnecessarily collected children's e-mail addresses and passwords. Then stored them in an unencrypted format. Consider how much sensitive information you really need to collect and have a system in place to regularly delete out-of-date, unneeded information.

Limit the number of people who are able to access personal data. Only allow employees with a legitimate need-to-know access to sensitive data. In the FCC action against Twitter, they noted that most employees had wide-reaching and unnecessary access to customer data. Twitter failed to enforce password changes or automatic account lockouts after several failed login attempts for administrative passwords. These failures according to the FCC, made Twitter vulnerable to multiple hacks. Avoid Twitter's missteps by limiting access to sensitive data, requiring periodic password resets, and locking accounts after multiple failed login attempts.

Use industry-accepted encryption methods when storing and transmitting data. Data needs to be protected at all points of the transmission route. It is not enough to encrypt your server. If you need to transfer sensitive data, make sure that data is encrypted during transmission. This includes data stored on mobile devices (i.e., laptops, hard drives, etc...). A data breach involving the social security numbers, disability ratings, and other personal information of 26.5 million veterans occurred because a Department of Veterans Affairs analyst had his laptop stolen. Incidents like this can be avoided by encrypting the data during storage and requiring user authentication at all points of access.

Have a response plan in place. Developing a data-breach incident plan can protect county employees and data. Part of your incident plan should involve regularly backing up critical data. In a recent case involving ransomware, a CTSI member lost crucial data because they did not regularly back up their files to a separate secure location.

What This Means for Counties

In case of a data breach, contact the CTSI property and liability claims department immediately for help with an assessment of your exposure and for the critical next steps. As a CAPP member, your county has coverage in place to help manage the loss, and navigate the legal and digital steps to take after a breach occurs. For more information, contact CTSI at 303-861-0507.