TECHNICAL UPDATE

CTSI
Serving Colorado's Counties

Volume 27 Number 21 May 23, 2023

How Secure is Your Data?

Personal data has increasingly become a target of hackers. 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. Taking the necessary steps to protect personal data protects you from a data breach's public relations and legal consequences.

LIMIT THE DATA COLLECTED

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. They then stored the addresses in an unencrypted format. Consider how much sensitive information you really need to collect and have a system in place to delete out-of-date, unneeded information regularly.

LIMIT ACCESS TO DATA

Limit the number of people who can access personal data. Only allow employees with legitimate need-to-know access to sensitive data. The FCC action against Twitter 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. According to the FCC, these failures 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.

ENCRYPT DATA

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.

CREATE A DATA-BREACH RESPONSE PLAN

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 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.

800 N Grant St, Suite 400
Denver, CO 80203
(303) 861-0507
Fax: (303) 861-2832