Data breach exposes personal information of thousands of LAPD officers and applicants

July 31 2019, by Madeline Purdue

Credit: CC0 Public Domain

What happens when those who serve and protect are not being protected themselves? Officers at the Los Angeles Police Department found out recently after a data breach of the city's personnel department exposed

personal information of about 2,500 officers.

The breach also exposed the information of 17,500 officer applicants. The information exposed included "names, date of birth, part of their employee serial number and the email address and password they set up when applying for the job," according to NBC Los Angeles.

Los Angeles Mayor Eric Garcetti said the breach was discovered July 25 and "involved limited information about City of Los Angeles job applicants in a database that is no longer used by the Personnel Department," noting the city's Information Technology Agency has added additional layers of security to avoid similar breaches in the future.

The city and the LAPD did not say what caused the data breach.

The Los Angeles Police Protective League Board of Directors, the union that represents LAPD officers, called the breach a "serious security issue."

"We urge the City of Los Angeles to fully investigate this lapse in security and to put in place the strongest measures possible to avoid further breaches in the future. We also call upon the city to provide the necessary resources and assistance to any impacted officer who may become the victim of identity theft as a result of this negligence so that they may restore their credit and/or financial standing," said the LAPPL in a statement.

Greg Pollock, vice president of product at UpGuard cybersecurity company, warns against giving information to third party vendors.

"The problem of protecting personal data ... is that individuals cannot safeguard their information after it has been shared with a third party,"

said Pollock. While there's the option to not give info to organizations with security issues, "for job applicants, there is no alternative but to supply personal information to a third party."

Pollock says, instead, the responsibility lies with the people who are collecting the information to protect it.

"Because this is a widespread problem, there are emerging solutions, like the California Consumer Privacy Act, which provides incentives for organizations to reduce their risk both by collecting less information and by storing it more securely."

The LAPD says it is working to ensure its data is protected from further breaches. It also notified those who were affected by the breach and will update them throughout the investigation.

"The Los Angeles Police Department is working with our city partners to better understand the extent and impact of this data breach," the LAPD said in a statement. "Data security is paramount at the Los Angeles Police Department and we are committed to protecting the privacy of anyone who is associated with our agency."

A message sent to officers encouraged them to monitor their personal financial accounts, get copies of their credit reports and file a complaint with the Federal Trade Commission, according to NBC Los Angeles.