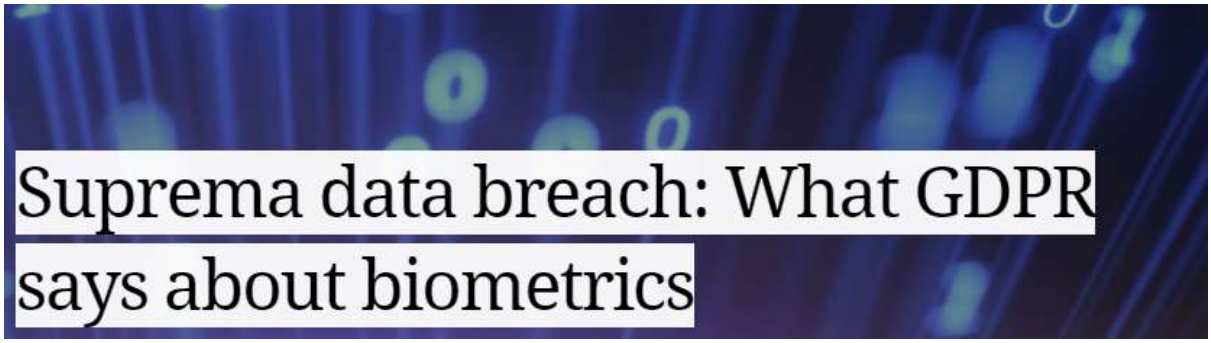
VERDICT



Robert Scammell – 15th August 2019 1:22PM

The Suprema data breach, in which researchers say they discovered the fingerprints, voice data, facial images, unencrypted usernames and passwords of more than one million people was publicly available, has drawn the condemnation of security experts and data privacy experts.

Israeli security researchers Noam Rotem and Ran Locar, along with privacy site vpnmentor, discovered that Suprema's BioStar 2 web-based security platform had left its database unprotected and mostly unencrypted.

The cloud platform holds the biometric data of people to grant them access to secure facilities in some 1.5 million locations around the world. According to the Guardian, the UK's Metropolitan Police force, as well as financial institutions, use the Korea-based firm's biometric platform.

In addition to the biometric data, the researchers were able to access the personal information of employees. In total, the pair had access to over 27.8m records, or 23 gigabytes-worth of data.

Rotem told the Guardian that they were able to access the plain-text passwords of administrator accounts, which meant an attacker could have added their own fingerprint to the account to then access the building.

TechCrunch's security editor Zack Whittaker called the researchers findings into question, tweeting that he had been unable to corroborate fingerprint data had been compromised.

Verdict reached out to Rotem, who said that it appeared Whittaker had made a mistake in his verification: "It seems they sent the wrong body in the request, it happens".

Clarifying the exact nature of the exposed data has been made more difficult by Suprema's unresponsiveness to the media and the researchers.

Suprema's head of marketing, Andy Ahn, told the *Guardian:* "If there has been any definite threat on our products and/or services, we will take immediate actions and make appropriate announcements to protect our customers' valuable businesses and assets."

Rotem told Verdict that Suprema's attitude "is very strange" and that since the story became public they have only received one email from a Suprema employee "thanking us for the disclosure, but nothing else".

Reaction to the Suprema data breach

Cybersecurity experts have stressed the serious implications of the Suprema data breach.

"You can't change your voice; you can't replace your eyes and you can't reset your fingerprints," said Etienne Greeff, chief technology officer at cybersecurity services and solutions provider

SecureData. “Those things are constant, permanent and contain genetic data that is unique to you.”

Failing to hash the data – a common security practice to hide sensitive information – and storing it on a publicly accessible cloud database amounted to “atrocious security practice”, he added.

“A significant element of this breach is the nature of how the biometric data was being used; to grant access to secure areas, for example in police stations,” said Stuart Reed, vice president of cyber at Nominet.

“Unlike many other cyber incidents that we’ve seen which compromise digital data, this breach directly crosses over into physical security, demonstrating just how dangerous the data could be in the wrong hands.”

GDPR & biometric data

Although there is no evidence that the biometric data was compromised by malicious hackers, the incident will likely constitute as a breach under GDPR.

“Researchers, by demonstrating a flaw, may be causing a personal data breach,” said data protection expert Robert Wassall, director of legal services at cybersecurity firm ThinkMarble.

Demonstrating a flaw on an unauthorised basis – as the researchers did – means “liability under the GDPR would rest with the ‘controller’ (usually the organisation being demonstrated to),” he added. “It would be up to the ICO to decide how to treat that breach.”

The ICO defines a personal data breach as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data”.

“In other words,” said Wassall, “the fact that no data was stolen is irrelevant.”

Under GDPR, biometric data falls under a special category that affords to extra protections.

“For many companies, this means that they may need to get consent from every person scanned

and prove that these individuals were fully informed and have given consent freely, without pressure or being penalised for not participating," said Tamara Quinn, partner at international law firm Osborne Clarke.

The ICO recently said that, for the rest of this year, it plans to focus on how organisations understand the risks associated with the way they process data.

If the ICO were to conclude that Suprema had failed to protect the data of EU citizens, the firm could face a maximum fine of up to 4% of global annual turnover.

"In the matter under consideration, the question is did Suprema understand the risks to people and can they demonstrate that these risks were taken into consideration (and mitigated)?" said Wassall.

"If Suprema is found to have breached the GDPR I would anticipate there is a high likelihood of a fine," he added.

An ICO spokesperson told Verdict that it is "aware of media reports in relation to this matter and we will be making enquiries".