Unit 10 Seminar

Data breach case study : MyFitnessPal

Jonathan Callaghan

1 February 2022

Breach checklist

What type of data were affected?

What happened and who was responsible?

Were there any escalation(s) stopped - how?

Was the Business Continuity Plan instigated?

Was the ICO and affected individuals notified?

What were the social, legal and ethical implications of the decisions made?

If you were an ISM for the organisation, what mitigations would you have put in place to stop any reoccurences?

What type of data were affected?

The affected information included:
IP addresses
Usernames
Email addresses
Hashed passwords - the majority with the hashing function called bcrypt used to secure passwords.

Bcrypt is a password hashing mechanism that incorporates security features, including multiple rounds of computation, to provide advanced protection against password cracking

The MyFitnessPal account information that was not protected using bcrypt was protected with SHA-1, a 160-bit hashing function. (Earlier accounts)

What happened and who was responsible?

What happened?

Shares dropped 3.8% ↓

On March 25, 2018, Under Armour MyFitnessPal became aware that on 1st February of this 2018 an unauthorized party acquired data associated with MyFitnessPal user accounts.

Who was responsible?

At time of press release they claimed they did not know.

After the release of data in February 2019 on Dream Market cyber-souk located in the Tor network, a source requested on HIBP the data to be attributed to BenjaminBlue@exploit.im

Were there any escalation(s) stopped - how?

143,606,147

Users

Feb 2019 – credentials appeared on the dark web along with 15 other website for ≈ $20,000 BTC

+ve

Data

The security was able to protect birthdays, location and credit card details from being exposed.

Encryption

Bcrypt: More robust but slow with layers of defence to make the process difficult to reverse.
SHA-1: Flaws and discredited but fast withfew resources needed and simpler for developers.

Was the Business Continuity Plan instigated?

Yes, however UA kept the data compartmentalised that allowed to keep data separated from other types of data such as payment information.

Was the ICO and affected individuals notified?

ICO

No decision notice on ICO site however users have been encouraged to contact ICO if they have a complaint.

Users

Notified on 29 March 2018

Recommended to:

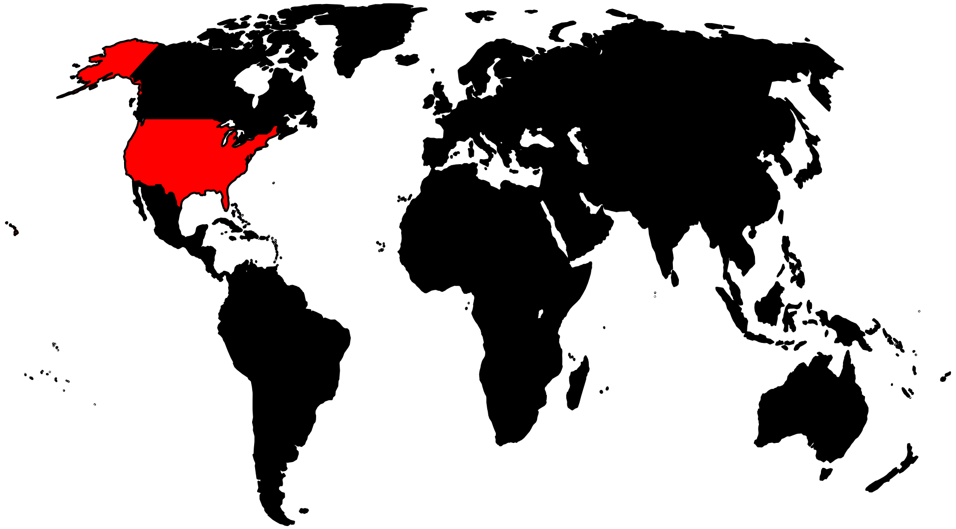
Change the password and for any other account with the same or similar information used.

Review accounts for suspicious activity.

Be cautious of unsolicited communications that ask for personal data and refer you to a web page for this.

Avoid clicking on links or downlaoding attachments from suspicious emails

What were the social, legal and ethical implications of the decisions made?



US Federal Court case

Rebecca Elizabeth Murray v. Under Armour Inc. Case No. 2:18-cv-04032

Murray claims that the company did not take sufficient steps to protect consumer information. Sought damages for herself and all similarly affected consumers, claiming that she was financially injured by the breach.

Murray claims that the company failed to notify consumers of the data breach in a timely manner. Allegedly, their delay in notifying consumers of the breach magnified the damage done, because it prevented consumers from taking action quickly to minimise the damage done by having their information stolen.

HIPAA

Health mobile apps are not covered within HIPAA

UA sought for arbitration arguing all users are required to accept the terms and conditions before using the app. Judge suggested this is a ‘clipwrap’ agreement and was sufficient whilst the T&Cs were held within the American Arbitration Association Rules.

If you were an ISM for the organisation, what mitigations would you have put in place to stop any reoccurrences?

Audit

Vet and audit the security protections in place.

Risk

Asses which elements of the app could raise risk.

Provide a security feature list as guideline for implementation

BCP

Review the Business Continuity Plan with list of actions to implement in a given scenario.

ISO 22301 compliant business continuity plan

Report

Describe the level of security needed with recommendations.

In recovery (Bitner et al 2006):
Recognition
Explanation
Apology
Compensation

Mitigations

Enhanced detection

Token validation for users

Encryption of all data through local database and cache

Multi layered authentication

Secure code development

References:

Bitner, M.J., Booms, B.H., Tetreault, 2006, M.S.: The Service Encounter: Diagnosing Favorable and Unfavorable Incidents. J. Mark. 54, 71 (2006)

Newcomb A., 2019, Hacked MyFitnessPal Data Goes on Sale on the Dark Web—One Year After the Breach *https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach* Date accessed: 1 February 2022

Under Armour, 2018, MyFitnessPal Account Security Issue, *https://content.myfitnesspal.com/security-information/FAQ.html* Date accessed: 1 February 2022