

Beacon CRM Cyber Security Incident

What organisations should do now



What has happened?

Beacon CRM, a widely used CRM platform within the UK charity sector, has reported a cyber security incident. Publicly available information indicates that database backups may have been accessed by an unauthorised party.

While current reports suggest that passwords and payment card details were not exposed, personal and organisational data may have been affected. This incident highlights the growing risk posed by third-party and supply chain cyber-attacks. This document sets out actions your Incident Management Team should consider when responding to the incident.

Actions we recommend

1. Stay informed
 - Monitor updates, guidance and recommended actions issued by Beacon.
 - Maintain a record of decisions and actions taken by your organisation in response to the incident.
2. Understand your exposure
 - Identify what information your organisation stores within Beacon.
 - Assess potential impacts on individual donors, volunteers, employees, trustees and partners.
3. Review data protection obligations
 - Assess whether the incident presents a risk to any of the affected individuals.
 - Assess and document if any UK GDPR and ICO notifications are required.
 - Seek advice from your Data Protection Officer or legal advisors if necessary.
4. Be alert to follow-on attacks
 - Expect an increase in phishing, impersonation and Business Email Compromise (BEC) attempts.
 - Remind staff, volunteers and trustees to be vigilant and verify unusual requests, payment changes and any unexpected emails.
5. Strengthen account security
 - Review Beacon user accounts and permissions.
 - Consider changing passwords for user accounts associated with Beacon.
 - Enable Multi-Factor Authentication (MFA) wherever available.

6. Review connected systems
 - Identify which other systems Beacon is integrated with, such as fundraising, marketing, finance or volunteer management systems.
 - Assess if any additional data may have been exposed via connected systems.
 - Review access permissions between any systems connected to Beacon CRM.
7. Review supplier arrangements
 - Review contracts and data processing agreements with Beacon to understand:
 - Data breach notification obligations
 - Data processing responsibilities
 - Liability provisions
 - Incident response commitments
 - Forensic investigation and remediation support arrangements

Key lessons

This incident demonstrates that even organisations with strong internal controls can be affected by cyber-attacks on trusted third-party suppliers. Organisations should consider strengthening:

- Third-party and supply chain risk management.
- Incident response plans.
- Crisis management and tabletop exercises.
- Cyber security awareness training.

How Zurich Resilience Solutions can help

Zurich Resilience Solutions can support organisations with cyber resilience reviews, third-party risk assessments, Cyber Health Checks, incident response planning, cyber risk quantification and crisis simulation exercises.

If you would like to discuss the implications of this incident or strengthen your organisation's preparedness and resilience against similar cyber events, please contact your Zurich representative or email us at zrs.enquiries@uk.zurich.com

This document is based on public information available at the time of publication. Investigations remain ongoing and recommendations may change as further details emerge. This document has been produced solely for informational purposes. The information contained in this document has been compiled and obtained from sources believed to be reliable and credible, but no representation or warranty, express or implied, is made by any member company of the Zurich Insurance Group as to its accuracy or completeness. This document does not constitute, nor is it intended to be, legal, underwriting, financial, investment or any other type of professional advice. No member of Zurich Insurance Group accepts any liability arising from the use or distribution of this document, and information, liability whatsoever resulting from the use of or reliance upon this document is expressly disclaimed. Nothing expressed or implied in this document is intended to, and does not, create legal or contractual relations between the reader and any member company of the Zurich Insurance Group. Any opinions expressed herein are made as of the date of their release and are subject to change without notice. This document is not, nor is it intended to be, an advertisement of an insurance product or the solicitation of the purchase of any insurance product, and it does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.

Zurich Resilience Solutions UK
Risk Support Services
6th Floor, The Colmore Building
20 Colmore Circus, Queensway
Birmingham
B4 6AT

For further information about any of the topics mentioned in this document please speak to your local Zurich contact, or email Zurich Resilience Solutions at zrs.enquiries@uk.zurich.com or alternatively call this number +44 (0) 121 697 9131.

For more information, please visit <https://www.uk.zurichresilience.com>

Zurich Management Services Limited, Registered in England and Wales no. 2741053, Registered Office:
The Zurich Centre, 3000 Parkway, Whiteley, Fareham, Hampshire PO15 7JZ

©2026 Zurich