Beacon Cyber Security Incident Final Report

September 2026

Beacon

Table of Contents

1. Introduction from the Beacon founders

2. Summary of the incident

3. Immediate containment and eradication steps

4. Regulatory responsibilities and reporting

5. How are we ensuring that this doesn't happen again?

6. Beacon's long-term security strategy

7. Getting in touch with Beacon

Appendix 1: Technical description of the incident

Appendix 2: Independent review of containment and eradication measures

01/

Introduction from the Beacon founders

On the 29th of July we discovered some suspicious activity in our AWS (Amazon Web Services) environment. Within an hour, a team of specialists had been assembled and got to work.

Through our investigations, it became apparent that someone outside Beacon had gained access to our AWS account. What we now know is that they had used a stolen access key to make a copy of our entire database, containing all customer data that was stored in Beacon as of the 27th of July, and there is evidence to suggest that this copy was downloaded. All of the data stored in our systems is encrypted, but the kind of access this person had meant they could decrypt the data while downloading it.

We know what that means for you. It means work you hadn't planned for, and questions from your trustees and supporters that you couldn't fully answer.

The experts helped us to find a vulnerability that was the probable root cause, and we fixed it quickly. They have since checked that our fix worked and confirmed that there was no evidence of any further access to our systems.

We then changed every key that might have been compromised and made updates to, as best possible, make sure this couldn't happen again.

Even with the fix in place, we still didn't know exactly what had been taken. We decided it was better to inform you all of what we knew and suspected, than to wait until we had more information, so we contacted customers, the ICO, and law enforcement on the 3rd of August.

We decided the best way to answer questions would be the same way that customers usually get support from us: live chat and email. We gathered people from across our organisation to expand our support team capacity so that we could get answers to people quickly.

Which brings us to today. Our systems are secure and operating normally. Other than a few minutes of downtime to deploy the fix, we didn't experience any interruption to Beacon services.

We have not engaged with the threat actor, though they contacted us once towards the conclusion of our investigation, only to indicate they would be deleting any data they have exfiltrated and no copy would be retained, sold, or shared. Given these are criminal actors we did not respond and our work is uninfluenced by this message. Dark web monitoring has found no mention of this incident or data related to it online. There is no evidence that this was a targeted attack on Beacon, or any specific Beacon customer. We're passing everything we learn on to law enforcement.

In this report you will find sections to answer questions on the detail of what happened (section 2), as well as answers to the questions we get asked most often: Did we report this, what steps have we taken to make sure it never happens again, and what does the future of Beacon look like now?

We've included two appendices: The first is the most technical account of the incident that we can provide. The second is a letter of attestation from an independent security organisation who were not part of the investigation and who have checked our work.

Beacon is independently owned and financially stable. We have always taken the approach of planning sensibly for the future and ensuring that our organisation is sufficiently resilient that we can weather challenging times.

Whilst this incident has come at some financial cost, we remain in a strong commercial position and have both an exceptional team in place and a solid product roadmap.

Beacon will continue to grow as a product and as an organisation, due to the measures that were in place before this incident, and due to our resolve to continue to serve the charity sector. We both designed and built this company to last, and we're both still here doing the work.

To all customers, we'd like to thank you for your understanding and patience as we've worked through this incident. Keeping your data secure is the most important thing we do at Beacon, and we recognise the serious impact this incident has had on your organisations.

Chris Houghton
Chief Executive Officer

David Simpson
Chief Technology Officer

02/

Summary of the incident

This summary provides an overview of the incident and is intended for non-technical team members, management, and trustees. For those interested in more detail with more specific language, a more technical summary is included in Appendix 1.

What happened?

In July 2026, we experienced a cyber-security incident in which an unauthorised third party gained access to our systems. We acted quickly to identify the threat, contain it, and eradicate the vulnerability.

Our investigation has concluded that an unauthorised third-party gained access to our system on 27 July 2026 at 01:20:16 UTC. Shortly afterwards, our findings indicate that:

- A copy of our database, which holds all Beacon customer data, was made.
- There was a significant increase in data transfer - suggesting substantial downloads occurred.
- There is no evidence to show exactly what these downloads contained.
- The volume of the data transfer suggests that the unauthorised third-party may have exported the entire database, containing all data and attachment files for all customers.
- Whilst the data was encrypted at rest, the threat actor had valid credentials, and therefore the download process would have decrypted the data.
- There is no evidence that any payment details from payment processors have been compromised.

We have not engaged with the threat actor, though they contacted us once towards the conclusion of our investigation, only to indicate they would be deleting any data they have exfiltrated and no copy would be retained, sold, or shared. Given these are criminal actors we did not respond and our work is uninfluenced by this message.

Dark web monitoring has found no mention of this incident or data related to it online.

There is no evidence that this was a targeted attack on Beacon, or any specific Beacon customer.

How it happened

The probable root cause of this incident was a compromised AWS access key. Such "access keys" are credentials used to allow the Beacon application to communicate securely with Amazon Web Services, our primary cloud hosting provider. This wasn't as straightforward as someone's username and password being hacked.

Our understanding is that this access key was inadvertently exposed in our application code and was subsequently used to gain unauthorised access to our AWS environment.

Our immediate actions

We immediately brought in independent expert cyber-security support to assist our engineering team with containment and eradication.

The vulnerability that enabled this exploit has been remediated, and we have implemented multiple checks to ensure this cannot happen again. Some of these measures, along with our plans for the future, are detailed later in this report.

After containing the initial incident and eradicating the likely root cause, no further suspicious activity or ongoing unauthorised access to our systems has been identified. Control Risks, our third-party cyber-security experts, have verified that our eradication work has been effective in containing the incident following no further indications of unauthorised access. More recently, we engaged another third-party cyber-security team to double check these findings. The results of this second review can be found in Appendix 2.

Security at Beacon before the incident

We take security incredibly seriously at Beacon and have invested a great deal in security to date. While this incident has reinforced that security is continually evolving, we already maintain strong security measures, including:

- ISO 27001:2022 UKAS accredited certification (last audit: June 2026)
- Cyber Essentials Plus certification (last audit: November 2025)
- Annual penetration testing (most recent test: March 2026)
- Encryption (AES-256 industry standard, TLS 1.2)
- Access controls and user permission management
- Dependency scanning
- Vulnerability remediation processes and SLAs
- AI code reviews followed by human code reviews
- Employee security training (every 6 months)
- Extensive information security policies

For a full list of technical measures currently implemented, we can share the latest version of our separate Beacon Security Practices document.

Current security status at Beacon

Beacon is fully operational and working as normal. Beyond our immediate containment actions, Beacon hasn't experienced any service interruption as a result of this incident.

Our external cyber security experts have been able to confirm that, since containing the initial incident, they have not identified or observed any ongoing unauthorised access to Beacon's AWS environment or engineer endpoints.

03/

Immediate containment and eradication steps

Our understanding is that a compromised AWS (Amazon Web Services) access key was used to gain access to Beacon. This was more sophisticated than a simple compromised username and password. More technically, the probable root cause of this incident was a compromised AWS access key which was potentially exposed in public JavaScript build artefacts in the Beacon application.

Having identified the probable root cause of this unauthorised access, we fixed the vulnerability quickly. The effectiveness of this fix was reviewed and confirmed by external cyber-security experts.

Next, out of an abundance of caution, we cycled all keys and credentials that could have hypothetically been compromised, including requiring the resetting of all passwords and app-based 2-factor authentication for all users.

Finally, our external cyber-security experts forensically inspected our systems for any other signs of compromise. They installed their own endpoint and cloud security systems on top of ours, so they could independently check for any "Indicators of Compromise."

Since containing the initial incident and eradicating the likely root cause, no suspicious activity or ongoing unauthorised access to Beacon's AWS environment or engineer endpoints have been identified. No methods of persistence used by the threat actor to maintain access to the AWS environment have been identified.

Given the identification of a probable root cause, its eradication, and following a review by cyber-security experts that did not identify any other vulnerabilities as a result of this incident, Beacon's engineering team are confident that the incident is resolved.

To provide extra reassurance of the efficacy of our containment and eradication measures, we have commissioned a separate independent third-party report which can be found in Appendix 2.

04/

Regulatory responsibilities and reporting

We consider it absolutely crucial that we engage with law enforcement, and to go above and beyond in our reporting responsibilities to regulatory authorities.

We pre-emptively reported this incident to the ICO on Monday 3rd August 2026, while our investigation was ongoing and before we were legally required to do so. Our reference number is IC/0238/2026.

We also reported this incident to all of our customers on Monday 3rd August 2026. This meant that we didn't have a lot of information to share from our investigation at the time of our first announcement, which many customers found frustrating.

Given that we needed our customers to take action to reset passwords and to reconnect apps, we decided that it was right to report the incident before we had completed our investigation and provide updates via our website and Facebook community as we learned more, rather than waiting until we had more information about the incident. We ensured that we had extra team members available to answer customer questions via live chat and email.

We also reported to law enforcement and have been helping The National Crime Agency and The Metropolitan Police with their investigations. Our crime reference number is RF26080356093C.

We have been in contact with The Charity Commission and have co-operated with their requests for information.

Maintaining our ISO27001 certification requires that we log this incident internally in our Information Security Event Log. This incident, and our response to it, will be reviewed by auditors as part of our next annual surveillance audit in June 2027.

05/

How are we ensuring this doesn't happen again?

Security is about layers. The Swiss Cheese Model is a helpful way to think about building secure systems. Every security mechanism is imperfect and will have some holes, much like a slice of Swiss cheese. The solution is to take a layered approach to security, placing several different slices on top of each other. Now it's far less likely that the holes will all line up, and we have built a more robust security system from imperfect slices. Typically, if things go wrong, you'll find that a combination of multiple smaller things have gone wrong in sequence.

Whilst we had strong security measures in place, given the evolving landscape and from the analysis of the probable root cause of this incident, we have added some new layers to do our utmost to prevent this from happening again. We have also reviewed several existing layers, and made improvements to them where necessary. By making small improvements throughout our security stack, we ensure a more robust security position than we can achieve through any single large change.

These are the layers that we've added, updated, or reviewed to ensure that this vulnerability cannot be exploited in the future:

Joint human and AI code review system

Every line of code that we deploy is double-checked by a different engineer from the one who wrote it, and an AI-based system does a final security check before going live.

Automated scanning of codebase for keys

Beacon's codebase is regularly scanned for exposed keys. An AWS key exposed in source code would trigger an alarm.

Automated scanning of build artefacts

Beacon's build artefacts are scanned for vulnerabilities before they are deployed to our production environment. An AWS key exposed in a build artefact would block the deployment.

Key management system for deployments

Beacon does not use static AWS access keys for deployments, making use of the OIDC identity verification layer instead. The vulnerability that was exploited in this incident required a static AWS access key, and we no longer use static AWS access keys at all in our build and deployment process.

Increasing the cadence of manual penetration testing

ISO27001 requires annual penetration testing. We have increased the frequency of our penetration testing to every 6 months in March and September. September tests will be carried out by the same provider, and March tests will cycle through different providers. This will ensure more eyes are on the Beacon system.

Continuous automated penetration testing

To stay ahead of evolving threats, we are also introducing continuous penetration testing, in addition to our annual tests. A vetted community of ethical hackers and AI agents will constantly probe our defences year-round, allowing us to identify and patch security gaps in real-time.

Third-party security assessments

We are engaging independent cybersecurity consultants annually to review our security posture. These experts will dive deep into our engineering practices, identify potential vulnerabilities, and ensure we benchmark against industry-leading best practices.

Crucially, they will also evaluate our incident readiness and response protocols, ensuring that our team is fully equipped to detect, contain, and resolve any future anomalies as swiftly and effectively as possible.

Staff responsibility and ownership

We have appointed a technical security champion within the engineering team to drive technical security initiatives. We have also appointed a release safety champion with responsibility for the security of the Beacon deployment process.

Our broader measures

Whilst we have shared details on the most relevant parts of our security system in this section, the list above isn't exhaustive. As you might understand, there are some specifics about our security measures, practices, and monitoring that we can't talk about to ensure their protection.

06/

Beacon's long-term security strategy

As a software company, one of our core values has always been focus. We do one thing and we do it well, and we don't build things just because we can. This incident is an opportunity for us to re-evaluate our focus and to ensure that we're concentrating on two key areas: Security and Product.

We try to embed security into the fabric of the Beacon product at all levels. While we do not intend to make any changes to our product roadmap, we absolutely will be working to lay out a long-term security roadmap for Beacon's future. This is a summary of our approach to security over the coming months and years.

Security certifications

We have learned from this incident that while rigorous security certifications are essential, they are not infallible. Our ability to respond to this incident effectively was in no small part due to the preparations put in place as required by ISO27001. We shall continue to maintain an Information Security Management System to the standard required by ISO27001 and ensure that this incident forms a part of improvements to that system. We shall continue to ensure that all audits are carried out by UKAS certified accreditation bodies.

We will also continue to maintain Cyber Essentials Plus certification. The specific endpoint testing that forms a part of this audit is valuable for verifying the setup of our devices.

We will continue to review whether SOC2 certification will significantly improve our security position, and undertake an appropriate audit process if we conclude that it will.

Staff

We will ensure that our security team scales with the organisation. We have a member of the team who undertakes a full-time security role, and we'll review whether we need additional security-focussed resources along the way. We've also appointed two security engineering champions and we'll be closely monitoring the efficacy of these roles. We'll prioritise making sure that we have the team members in post that we need in order to deliver on our security roadmap.

Alignment around security frameworks

To align our technical security efforts, we are adopting two globally recognised frameworks from the OWASP Foundation. These frameworks provide a structured way to continuously assess our security posture, track our maturity over time, and hold ourselves accountable to the highest industry standards.

- **Software Assurance Maturity Model (SAMM):** A strategic roadmap to guide how security is embedded into every stage of our software development lifecycle.

- **Application Security Verification Standard (ASVS)**: A rigorous technical blueprint providing clear controls to verify that every feature we build functions securely.

Consolidation of our authentication systems

We will bring our user authentication systems together under a single provider to streamline and simplify their development and maintenance. There are several well regarded industry standard providers in this space for us to choose from.

Customers will benefit directly from some of our authentication improvements and shared learnings. For example, we'll introduce SAML Single Sign-On. This will allow organisations to manage Beacon access through your central identity providers – enabling you to enforce strict global access policies and ensuring instant access revocation when an employee leaves, or in an emergency.

We will introduce Passkeys for the Beacon team. These replace passwords with device-based biometric logins. Initially, we'll roll these out for the engineering team, with the intention of introducing passkeys to all Beacon team members.

Working with experts

Our security compliance journey so far has been guided by a team of independent security consultants, who we will continue to engage with to ensure we are meeting the ongoing requirements for ISO27001, including running internal audits for us, and managing tests of business continuity scenarios.

We will engage with a new organisation to provide a comprehensive, independent security review of our systems every year. We have seen the value in bringing in external cyber-security experts to review our systems as part of our incident response and we will do more of this.

Advocacy

We believe that the charity sector will benefit from open conversations about security and rigorous debate. We want to help make a stronger and more resilient sector through thought leadership and sharing what we've learned.

07/

Getting in touch with Beacon

You can review our previous communications about this incident on our incident page at **https://www.beaconcrm.org/incident**.

We have a page of Frequently Asked Questions which you can find here: **https://www.beaconcrm.org/incident-faqs**.

Finally, we have a dedicated Security Incident Response Guide web page at **https://www.beaconcrm.org/incident-guidance** with recommended actions for affected organisations.

If you have further questions that can't be answered using these web pages then you can get in touch by emailing us at **incident@beaconcrm.org**. Our team will be here to help.

Appendix 1: Technical description of the incident

Initial access and root cause

The probable root cause of this incident was a compromised AWS access key which was potentially exposed in public JavaScript build artifacts. The earliest malicious activity observed so far occurred on 27 July 2026 at 01:20:16 UTC.

Data exfiltration assessment

Analysis of the AWS Cost & Usage reports across May-July 2026 has been conducted. This data showed a significant increase in data transfer on 27–28 July 2026. This timing correlates with the malicious activity, which supports an assessment that substantial downloads occurred. Specific objects, exact destination of the downloads, and definitive attribution of which objects were accessed cannot be determined from available logs. However, having reviewed the data transfer volume and the total volume of data stored across the system, our assessment is that the threat actor exported all data contained within the database.

The data was encrypted at rest in AWS, but the threat actor had valid credentials and therefore downloads would have been decrypted by AWS and available unencrypted to the threat actor.

Our assessment is that the threat actor exported all data contained within the Beacon database, so almost all accounts are affected. Only accounts that had been deleted more than 30 days before the 27th of July are not affected.

We have not engaged with the threat actor, though they contacted us once towards the conclusion of our investigation only to indicate they would be deleting any data they have exfiltrated and no copy would be retained, sold, or shared. Given these are criminal actors we did not respond and our work is uninfluenced by this message.

Dark web monitoring has found no mention of this incident or data related to it online. There is no evidence that this was a targeted attack on Beacon, or any specific Beacon customer.

Persistence

No methods of persistence used by the threat actor to maintain access to the AWS environment have been identified.

Having identified the most likely root cause of the unauthorised access, the vulnerability has been remediated and all credentials for services and accounts integrated with AWS reset.

Independent cyber security experts deployed SentinelOne Endpoint Detection and Response (EDR) and Cloud Native Security (CNS) across our environment and engineer endpoints, in addition to our existing security systems, to scan for Indicators of Compromise and suspicious activity.

Since containing the initial incident and remediating the likely root cause, no suspicious activity or ongoing unauthorised access to Beacon's AWS environment or engineer endpoints has been identified.

Appendix 2: Independent review of containment and eradication measures

Letter of Attestation

CYFOR Secure - Cyber Security

27 August 2026

Attn: The Board of Directors

Beacon CRM

Reference: 20260827-BEACON-LOA

Subject: Letter of Attestation - Independent review of the July 2026 security incident and the response to it

This letter is issued in my capacity as Head of Cyber at CYFOR Secure. It may be shared in full with Beacon CRM's customers and their own clients, and is intended to be read by a non-technical audience.

1. Why we were engaged

In July 2026 an unauthorised third party gained access to part of Beacon CRM's cloud environment. Beacon CRM responded in a reasonable time, brought in a specialist forensic team, and notified its customers, the Information Commissioner's Office, the National Crime Agency and the police.

Beacon CRM then asked CYFOR Secure to take an independent look. Our instruction was straightforward: examine what happened, examine what Beacon CRM did about it, and say plainly whether the response holds up. We are not connected to Beacon CRM beyond the fee for this work, and we have no relationship with the specialist team it appointed.

So that our view would be genuinely independent rather than a second opinion on someone else's, we rebuilt the picture from Beacon CRM's own system records rather than working from the earlier team's conclusions.

2. What we examined

Beacon CRM gave us read-only access to the affected environment. We could look at everything and change nothing, and at no point did we ask for or handle any of Beacon CRM's passwords or customer data.

Across three days we reviewed the administrative activity records for the environment, the accounts and access rights within it, the storage and database services, the systems that hold credentials, the security monitoring in place, and the configuration of the affected services. We compared all of it against the account Beacon CRM had given us and against the state of the environment as it stands today. Fifty-nine timestamped records of what we saw are held in our engagement file.

3. Our conclusion

> *Following an independent review of both the incident and the response to it, CYFOR Secure's professional conclusion is that Beacon CRM correctly identified how the unauthorised access occurred, closed it, removed everything the third party created within its systems, and replaced the credentials involved. We found no sign of unauthorised activity in the environment after 28 July 2026, and nothing left behind that would allow that access to be regained.*

Four points sit behind that conclusion, and each was verified by us directly rather than taken on trust.

The access route was shut. The credential that allowed the access was disabled on 29 July 2026 and the account it belonged to was deleted shortly afterwards. Nothing has used it since it was switched off.

Nothing was left behind. Everything the third party set up inside the environment has been removed. We checked specifically for the mechanisms an attacker commonly leaves in order to return later, and for any rule that would quietly continue copying data outwards. We found none.

Credentials were replaced quickly. The passwords and keys that could have been exposed were changed within days of the incident. Where our review identified older credentials that had been missed, Beacon CRM addressed every one of them within a day of us raising it.

The underlying issue was fixed properly. The way Beacon CRM's systems authenticate to its cloud environment has been rebuilt on a short-lived, per-service model. The arrangement now in place is materially stronger than the one that existed before the incident, and it removes the class of problem that caused it.

One further point deserves recording, because it speaks to how Beacon CRM approached this. Rather than confining its response to the data it knew had been touched, Beacon CRM treated all data held in its systems as potentially affected. It rotated credentials across the board, required every user to reset their password and re-register two factor authentication, and worked directly with its own customers to replace any third-party credentials that might have been caught up in the incident. That is a more thorough response than the circumstances strictly demanded, and in our view it was the right call.

4. Basis of this opinion

This letter concerns the incident of July 2026 and the response to it. It is not a penetration test, a security certification, or a general statement about Beacon CRM's systems, and it speaks to the position as at 27 August 2026.

One limitation should be stated, Beacon CRM's environment was not configured to record every individual file access at the time of the incident, which is a common configuration and not a failing peculiar to Beacon CRM. It means that whether the copies of data made by the third party were ultimately taken away cannot be proven either way, by us or another provider. Beacon CRM did not wait for that certainty. It assumed the data had been taken and notified its customers and the authorities on that basis, which is the cautious and correct position, and it is the reason this letter does not claim that no data was removed. We have recommended that Beacon CRM enable that additional level of logging, and it forms part of our technical report.

Our findings are drawn from Beacon CRM's own cloud records and configuration, together with the written account Beacon CRM provided. Where a statement in this letter rests on Beacon CRM's account rather than on our own examination, the technical report identifies it as such.

Beacon CRM approached this openly, gave us access to everything we asked for, and acted on every point we raised without argument or delay. On the evidence we examined, its customers can have confidence that this incident was properly understood, properly closed out, and has left the environment in a stronger position than it was in before.

Yours sincerely,

Luke Davis

Head of Cyber, CYFOR Secure

End of Letter of Attestation - Ref 20260827-BEACON-LOA.