

DARKBEAM SUPPORTED A LEGAL FIRM TO MEET THEIR DATA PROTECTION REGULATORY REQUIREMENTS

The Challenge

With limited in-house digital risk capabilities, the firm needed help understanding their digital footprint and cyber posture to understand how to mitigate threats posed from the digital world.

The firm had previously instructed a third-party provider to maintain its cyber posture and manage its digital assets, including maintaining its SSL certificates. It now needed reassurance that the work undertaken by the third-party met their expectations.

Our Solution

As the client needed instant assurances that their regulatory requirements were being met, Darkbeam generated a Digital Risk Report via the Darkbeam platform in under five seconds. By providing a hacker's eye view of the firm, the report identified the critical vulnerabilities that needed to be prioritised for remediation

The Results

The stakeholder summary of Darkbeam's Digital Risk Report instantly revealed that the firm did not have an SSL certificate deployed correctly. This lack of valid certification made it impossible for a secure connection to be formed between the client's domain and the browser of the person visiting the website. This type of lapse typically results in reputational damage but was particularly concerning in this case as the firm's website was used for clients to enter confidential information.

Allowing this sensitive information to be exposed is a breach of GDPR and without a valid SSL certificate this information was transmitted in plain text across the internet, making it an easy target for cybercriminals. As a result of Darkbeam's report, the law firm dispensed with the services of the third party and ensured that the SSL certificate was deployed correctly going forward, thereby ensuring GDPR compliance and protecting their clients.