Bark
Case Study

Service:

**Cyber Maturity
Assessment**

caseStudy

How Bark was able to fully understand its security posture and obtain cyber insurance with a Cyber Security Maturity Assessment

The Requirement

Bark is the UK's largest and fastest growing services marketplace, helping people find the right professional for their project in over 1,500 unique categories.

Bark has been connecting consumers and businesses with everyone from cleaning services to lawyers and accountants since 2014.

Bark is on a mission to revolutionise and become the leading online marketplace for professional services. They are passionate about helping people find what they need and helping the businesses that provide these services succeed and manage customers better.

Bark received investment from a private equity firm in 2022. As part of the investment process, the investors requested that Bark complete a cyber security assessment.

This would provide proof of existing security measures and confidence in a future security roadmap, so Bark and the new investors could obtain cyber insurance.

Bark
Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Cyber Maturity Assessment

caseStudy

The Solution

The investment firm went through the process of selecting a cyber security services company to conduct the assessment and engaged DigitalXRAID's experts with the Bark team.

Several steps had already been taken to implement processes and products at Bark. The cyber security maturity assessment would evaluate operational resilience and existing cyber security procedures aligned with the National Institute of Standards and Technology (NIST) Framework.

The DigitalXRAID team worked closely with departments across the business to understand the procedures already in place, conducted against the five key NIST domains, 23 categories and 108 subcategories. The assessment didn't just cover technical controls, but also resilience across people, process and technology for a truly holistic view.

DigitalXRAID assessed the existing risk register, controls and tooling that had been put in place to assess whether there were any gaps that hadn't been considered.

On completion of the assessment, DigitalXRAID supplied a comprehensive report which gave Bark a baseline of their current cyber maturity and risk levels. Resilience indicators in the report highlighted any areas of vulnerability, the potential impact of not having certain processes and products in place, and the recommended steps to reduce remaining risk to acceptable levels for the business.

The final report was suitable for sharing with senior management to raise awareness of cyber security and current risk at a board level, and with Bark's investors. It also gave a clear outline of what security measures were in place for Bark's cyber insurance provider to assess against.

Bark
Case Study

Service:

Cyber Maturity Assessment

caseStudy

> "The DigitalXRAID team have been really helpful every step of the way. They fully understood our unique business drivers and aims. They took time to understand exactly what was already in place and formalise existing processes, rather than reinvent them, which was appreciated across the business. It was invaluable to have DigitalXRAID's input on calls with our cyber insurance provider to give confidence that measures were in place and address and concerns immediately. That was instrumental in being able to secure the policy and keep premiums at a reasonable level."
>
> *Henry Searle, Head of Engineering, Bark*

The Results

The results of the cyber security maturity assessment have given Bark a baseline on existing security. The report provides guidance for a cyber security strategy directly aligned to strategic business goals.

The DigitalXRAID team has provided a clear corrective action plan to address any gaps. Bark has divided the plan across the different business areas and assigned ownership of any remediation efforts to ensure that addressing gaps is prioritised and actioned promptly.

Cyber security has now become much more visible within Bark. The whole of the business can get more involved in cyber security, with all departments understanding their role in keeping the company secure and what action to take should an employee or customer be negatively affected.