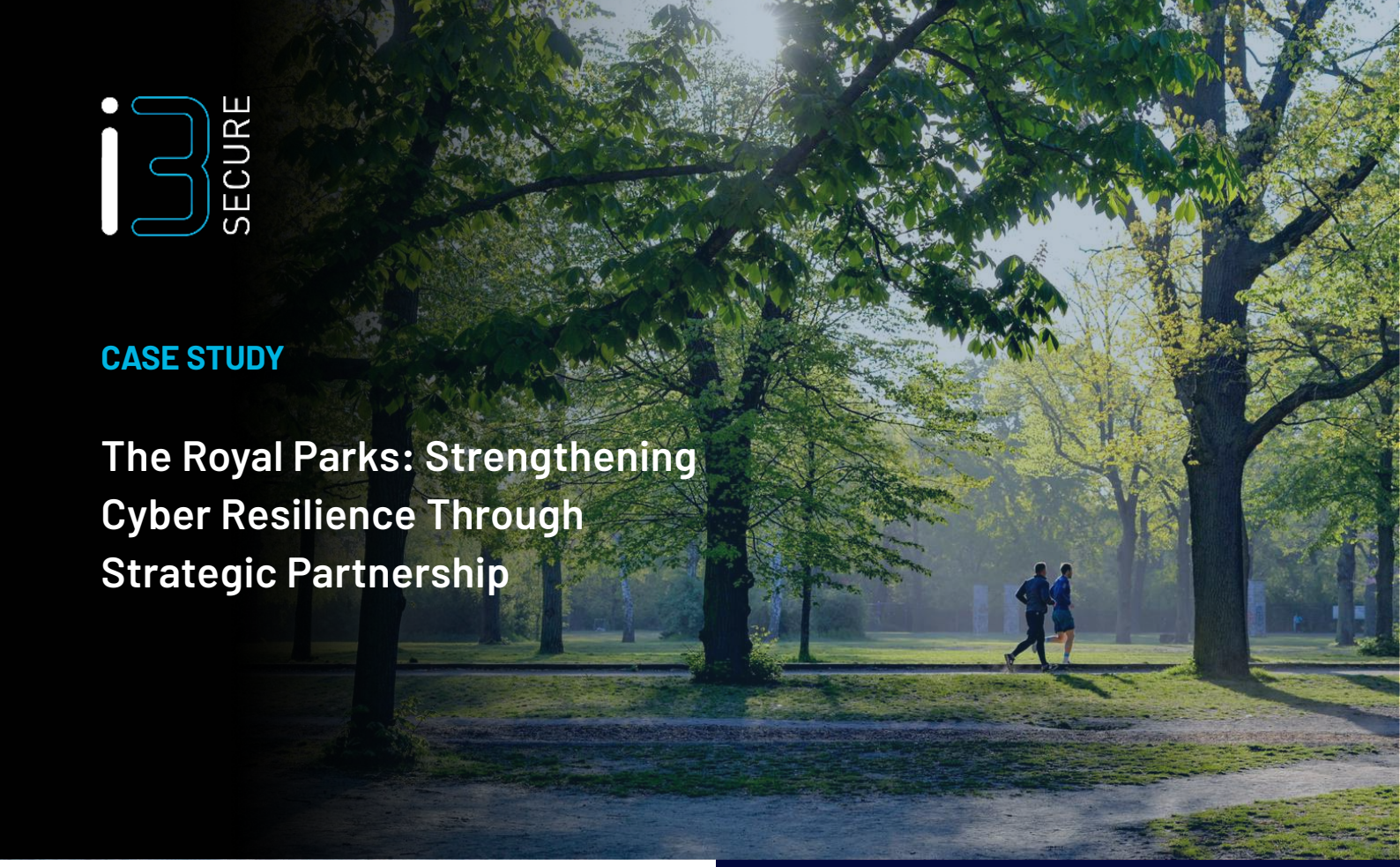

CASE STUDY

The Royal Parks: Strengthening Cyber Resilience Through Strategic Partnership

Overview

The Royal Parks (TRP) is a UK charity entrusted with the stewardship of over 5,000 acres of historic parkland in London, including Hyde Park, Regent's Park, and Richmond Park. Their digital infrastructure underpins a broad range of operational and public-facing services, from managing ecological data and staff operations, to facilitating events and supporting public engagement.

As part of a wider programme of strategic digital investment, TRP partnered with i3Secure to enhance their cyber security governance, align with recognised national frameworks such as NCSC's Cyber Assessment Framework (CAF), and build long-term resilience in an increasingly complex threat landscape.

The Challenge

Our consultants integrated seamlessly into TRP's organisational structure, collaborating with the IT department to deliver assurance based on Cyber and Information Security best practices.

Guided by their Head of IT, our team planned the project using accessible tools that enabled effective communication and progress reporting. Our consultants used tools such as Azure DevOps to structure the work into well-defined sprints and produced highlight reports to demonstrate completed tasks and the value delivered, ensuring full transparency and clear return on investment.

Our Subject Matter Experts selected the most appropriate cyber security framework to guide the project and measure progress. In tandem, we supported the IT Infrastructure Manager with technical expertise to deliver practical, business-ready solutions. To meet requirements, i3Secure deployed a well-rounded team of consultants with specialised skills in Governance, Risk, and Compliance as well as hands-on technical delivery.

© 2025 i3Secure Ltd

Our Solution

Laying the Foundations: Discovery and Assessment
To support TRP's long-term cybersecurity, i3Secure began with a comprehensive assessment using the NCSC's Cyber Assessment Framework (CAF). This identified TRP's strengths, weaknesses, and opportunities for improvement. We chose the CAF for its public sector alignment and enhanced it with ISO 27001 and Cyber Essentials principles to support TRP's broader compliance goals.

To guide the assessment, we created a bespoke, live gap analysis tool that tracked compliance and progress in real time. Based on the findings, we developed a prioritised roadmap of strategic recommendations to strengthen TRP's cybersecurity posture.

Delivering Cybersecurity Improvements
We followed the discovery phase with a custom NIST 800-30-based risk register to classify threats and guide mitigation, underpinned by ISO 27001. We established a Cyber Security Committee to oversee governance and enhanced core policies and procedures for greater control over network and application security.

To improve asset management, we introduced policies to track and maintain hardware and software with secure configurations. We strengthened application security through secure development practices and a formal review process. For supplier risk, we designed three questionnaires enabling TRP to assess third-party vendors regardless of contract size.

Endpoint protection was upgraded via antivirus reviews, access controls were tightened, and server and firewall settings were refined, especially in TRP's virtual environment.

Strengthening Resilience & Preparing for Certification
We validated TRP's continuity plans and developed a new, tested IT Recovery Plan. A cyber awareness programme featuring phishing tests, workshops, and e-learning boosted staff engagement, and a Cyber Security Steering Group was established for formal governance.

Incident response capabilities were enhanced with a new response plan, including a live brute-force simulation. Penetration testing (internal and external) also provided assurance and revealed additional vulnerabilities.

The Result

By acting on our consultants' recommendations, The Royal Parks significantly strengthened their security posture, achieved higher levels of regulatory compliance, and safeguarded sensitive data across their systems.

Their compliance with the NCSC Cyber Assessment Framework rose sharply from 61% to 95% for fully met controls—marking a substantial leap in cybersecurity maturity.

With core foundations now firmly in place—including robust risk management, auditing, incident response planning, business continuity strategies, and well-defined policies—TRP has gained greater confidence in its cyber resilience.

Our work also resulted in TRP having a clear roadmap toward Cyber Essentials and Cyber Essentials Plus certification, including an internal audit plan and actionable next steps.

This partnership has enabled The Royal Parks to build a more secure digital infrastructure, better prepared to withstand emerging threats and adapt to evolving regulatory and technological demands.

© 2025 i3Secure Ltd