Cyberfort
Expert-led. Security Driven.

Case Study

Discover how Morro Partnerships used Cyberfort Penetration Testing and Threat Intelligence services to ensure the companies cyber security posture is ready for future growth

Industry:
Property Management & Construction

Location:
United Kingdom

MORRO
Better *tomorrow* makers

Morro Partnerships is a leading affordable housing developer focused on building homes in the east and west midlands of the UK. With a significant history of building affordable homes and ambitious growth plans to build 4,000+ housing plots in the future, Morro Partnerships needed a cyber security provider who could provide them with the right services, skills and experience to support their growth ambitions and ensure their infrastructure, software and applications remained secure, resilient and compliant.

In this case study we examine how by engaging Cyberfort for penetration testing and threat modelling, Morro Partnerships could be confident in its future cyber security approach and be resilient against future threats.

The Challenge

Morro Partnerships had evolved significantly over the past 12 months. With its current and future growth plans making sure it had the right cyber security roadmap and strategy in place would be crucial for future business success.

The company's IT infrastructure had grown organically, with the internal IT team and several other IT service providers primarily focused on maintaining day-to-day operations. Their approach to security before engaging with Cyberfort was focused on traditional measures to remain secure against attack but was reactive in its approach.

Following the appointment of a new Group Technology Director – Jon Glover, they realised specialist cyber security support from a supplier who could give them independent advice on how to improve their current cyber security posture would enable them to develop a cyber security roadmap for the future.

Most crucially, Morro Partnerships board understood that cyber security wasn't simply about preventing attacks, it was about creating the foundation for trusted digital relationships with customers, partners, and investors that would enable their growth strategy.

The company reached out to Cyberfort as it had several cyber security challenges that it wanted to overcome and make sure it was ready for future growth. These included:

Legacy Systems and Technical Debt: Like many established home builders, Morro Partnerships had accumulated years of IT systems that had evolved organically rather than strategically. Their network infrastructure combined cloud-based project management tools, on-premises financial systems, and contractor portals had never undergone comprehensive security testing. The IT team did not have the time to identify vulnerabilities across this complex environment.

Supply Chain Complexity: Morro Partnerships operations involved coordination with suppliers, subcontractors, and professional consultants, each requiring different levels of system access. They needed to test the vulnerability of their interconnected supply chains in construction.

Regulatory and Insurance: It is well documented that insurers are now requiring evidence of robust cyber security measures, with premiums rising sharply for businesses unable to demonstrate adequate controls. Additionally, contracts with housing associations and public sector clients increasingly now mandate cyber security certifications signed off by independent third parties.

Customer Data Responsibility: With thousands of prospective buyers sharing financial information through their sales portal annually, and existing homeowners' details stored in their customer relationship management system, they needed to make sure the likelihood of data breaches were minimised and where potentially attackers were most likely to exploit security gaps in these systems.

Engaging with Cyberfort

Following an internal cyber security review Morro Partnerships contacted Cyberfort to discuss how their Penetration Testing and Theat Intelligent services could help them to assess their current cyber security position and provide them with a roadmap for future improvements.

Cyberfort proposed a phased engagement that would deliver immediate risk reduction while building toward comprehensive security maturity.

Over several weeks, Cyberfort's team conducted extensive penetration testing using CREST and CHECK accredited methodologies across Morro Partnerships digital infrastructure. Using the same techniques employed by malicious actors, they attempted to breach networks, access sensitive data, and disrupt systems. The testing covered all external infrastructure and was performed to identify vulnerabilities and strengths within the Morro Partnerships IT environment.

The results from the external infrastructure penetration test identified vulnerabilities and categorised them into which vulnerabilities were critical and should be acted upon first. Crucially, Cyberfort didn't simply provide a technical report. They translated findings into business impact scenarios which showed the potential costs and time delays if action was not taken.

In the next phase of work Cyberfort established a threat intelligence feed tailored to Morro Partnerships risk profile. This service monitored for compromised credentials, emerging ransomware variants targeting construction firms, and supply chain threats. Combining both Penetration Testing and Threat Intelligence streams Cyberfort worked with Morro Partnerships IT team to develop a prioritised remediation roadmap, categorising vulnerabilities by business impact and implementation complexity. They provided hands-on support for critical fixes while building internal capabilities for ongoing security management. This collaborative approach ensured that Morro Partnerships understood not just what to fix, but why it mattered and how to maintain security standards.

The Business Impact

Within the first 6 months into their partnership with Cyberfort, Morro Partnerships has experienced a range of cyber security benefits including:

- Enablement of Strategic Growth Initiatives - With a robust security foundation established, Morro Partnerships successfully launched several growth-enabling initiatives that would have been too risky previously.

- Insurance and Financial Benefits - Following Cyberfort's engagement and the implementation of their recommendations, Morro Partnerships is now in a place where they can evidence regular testing a cyber security roadmap to their insurers and regulators. In the future this will result in lower premiums and increased coverage limits, providing protection for scenarios that were previously excluded.

- Organisational Confidence and Culture - The partnership has elevated cyber security from an IT concern to a business priority. Board meetings now include regular security updates.

- Future-Proofing Through Continuous Improvement - Cyberfort continues to conduct regular penetration testing and provides monthly threat intelligence briefings. This continuous engagement ensures that as Morro Partnerships digital footprint expands and threat landscapes evolve, their security posture evolves in parallel. Recent testing confirmed that remediation efforts had eliminated several previously identified vulnerabilities, while catching new issues introduced through system updates before they could be exploited.

Lessons for other construction firms

Morro Partnerships experience offers valuable insights for similar organisations including:

- Recognising Security as a Growth Enabler - Cyber security shouldn't be viewed merely as protection against risk, but as the foundation enabling digital opportunities that drive growth and competitive advantage.
- Specialist Expertise Delivers Value - For mid-sized house building organisations, partnering with specialists provides capabilities and current intelligence that would be prohibitively expensive to develop internally, while offering scalability as the business grows.
- Business Context Matters - The most valuable security providers translate technical vulnerabilities into business impact, helping leadership make informed risk decisions aligned with strategic priorities.
- Continuous Engagement is Essential - Cyber security isn't a point-in-time exercise. Continuous testing and threat intelligence ensure that protection evolves alongside both the business and the threat landscape.

"Working with Cyberfort wasn't just about protecting what we'd built, it was about making possible what we wanted to accomplish as a company in the forthcoming years. That's been the real value. The Cyberfort team have helped us to supplement our existing skills with their specialist expertise which has helped us to develop a future cyber security roadmap matching the company's future growth plans. What has been most impressive is how the Cyberfort team have turned cyber security into a strategic workstream aligned to business priorities and KPI's. Through their detailed testing, reporting, threat intelligence and recommendations we can now clearly see what we need to focus on in terms of remediation and ensure it is part of our cyber security roadmap."

Jon Glover, Group Technology Director, Morro Partnerships

Final Thoughts

Morro Partnerships ongoing engagement with Cyberfort demonstrates how mid-sized house building organisations can transform cyber security from an ad-hoc exercise and compliance burden into a strategic asset. By engaging specialists who understood both the technical landscape and the business context, Morro Partnerships built the security foundation necessary to pursue ambitious growth plans with confidence.

As the house building sector becomes increasingly digital, with building information modelling, supply chain integration, and smart technologies becoming standard rather than exceptional, robust cyber security will separate leaders from the rest of the market. Morro Partnerships proactive approach has positioned them not just to defend against current threats, but to embrace future opportunities in an increasingly connected industry.