Article

Jan 2025

What is physical penetration testing and how can it help my business?

Physical penetration testing is a method used to assess the security processes and protocols of an organisation. It involves evaluating the effectiveness of physical security controls and staff compliance with security procedures, with a goal to determine whether a company is vulnerable to threats, both internal and external.

Simon Evans
Principal Security Consultant
Email simon.evans@waterstons.com

By simulating real-world attacks, pen testing helps validate the robustness of existing security measures or newly implemented controls after improvements. It reveals how secure or accessible an organisation is to potential attackers, allowing for corrective action to mitigate risks.

Why do companies need it?

In today's rapidly evolving threat landscape, companies face growing risks not only from cybercriminals, but also malicious insiders and physical security breaches.

Physical penetration testing provides the following:

- Opportunities to identify and resolve weaknesses before they are exploited
- Ensure regulations and compliance standards are met, such as GDPR, ISO 27001, and PCI DSS
- Ensures that sensitive data and assets are protected from breaches
- Uncovers blind spots in security, strengthens defences, and instils confidence that their security measures can withstand real-world threats.

Benefits of penetration testing

While we know what it does and why we do it, understanding what it can achieve for you and the benefits you will see from investing it are sometimes missed.

Here are a few of the benefits you will see from physical pen testing:

- Identifies security gaps and vulnerabilities in physical and digital security systems.
- Provides insight into the effectiveness of security protocols and employee compliance.
- Helps ensure compliance with industry regulations and standards.
- Strengthens the overall security posture of the organisation.
- Simulates real-world attacks to improve incident response strategies.
- Builds stakeholder confidence in the organisation's security efforts.

Risks of penetration testing

Even with its great benefits, physical penetration testing does not come without its risks, and these are important to understand and acknowledge before starting any test.

- Potential disruption to normal business operations during testing.
- False sense of security if testing scope is too narrow or incomplete.
- Miscommunication leading to unintentional triggering of alarms or defensive measures.
- Failure to remediate identified vulnerabilities can leave the organisation exposed.
- Legal or regulatory issues if testing is not properly authorised or breaches data protection laws.
- Financial costs associated with hiring specialised penetration testers.
- Damage to the company’s reputation if sensitive weaknesses are leaked or exploited during testing.

Physical penetration testing is a crucial tool for organisations to assess their security vulnerabilities and ensure their defences are effective. By balancing the benefits and risks, companies can use penetration testing to proactively strengthen their security and safeguard against potential threats from both internal and external sources.

For more information on the physical penetration testing services we offer, email Simon Evans at simon.evans@waterstons.com