

RICOH
CYBERSECURITY

Penetration
Testing



THE BUSINESS CHALLENGE

HOW TO AVOID A PUBLIC AND DAMAGING CYBER BREACH

Cyber crime is a growing industry, with criminals exploiting poor cybersecurity defences for large profits; putting business and customer data at risk. Inadequate security defences increase the likelihood of a successful attack.

The consequences of a cyber attack can be extremely damaging and include:


- Loss of revenue and/or customers
- Reputational damage
- Financial penalties from authorities
- Theft of intellectual property and sensitive company or customer data
- Unprecedented disruption to business-critical systems

When a business experiences a security breach, its customers and partners want to understand the impact of the attack and how it occurred. Meanwhile, regulators will scrutinise cybersecurity defences and response actions to determine fault and enforce appropriate penalties. By taking proactive steps to build a sound cybersecurity posture, your business can limit the financial consequences of an attack significantly.

Regular penetration testing reduces risk and demonstrates due diligence.

CYBERSECURITY BUSINESS OBJECTIVES

- Increase protection of business and customer data
- Reduce exposure to common and advanced cyber attacks
- Future-proof defences against preventable cyber attacks
- Limit exposure to legal and regulatory fines
- Meet compliance standards



RICOH Penetration Testing
identifies security weaknesses
and reduces risk



OUR SOLUTION

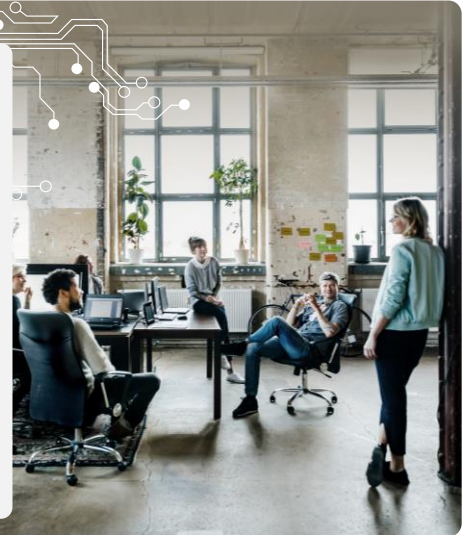
PENETRATION TESTING MIMICS A REAL CYBER ATTACK

Completing regular penetration testing as part of an ongoing risk management regime significantly reduces business exposure to cyber attacks and their impact.

Ricoh's global penetration testing services are designed to replicate both common and sophisticated cyber attacks.

We combine penetration testing with a range of capabilities to assess risk and defend against cyber threats. This includes providing a formal report with detailed recommendations to address vulnerabilities, along with remediation actions tailored to business needs.

The outcome is a solution that supports stringent compliance and legal standards across global regulatory regimes.

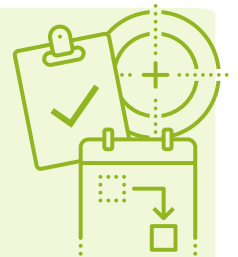


KEY OUTCOMES

A clear view of security weaknesses and exposure to attacks

Recommendations to close security holes prioritised in terms of greatest impact

Benchmarking against industry standards



Evidence that demonstrates responsible cybersecurity behaviours for authorities or regulators in the event of a breach

Tailored help with remediation to ensure all vulnerabilities are fixed (and verified as correctly fixed)

OUR EXPERTISE



Our penetration testing team is certified by the UK National Cyber Security Centre (NCSC) Check Scheme (UK Government), the independent Council for Registered Ethical Security Testers (CREST) scheme and the NCSC Cyber Essentials Scheme.



All our consultants hold NCSC CHECK Team Leader, Check Team Member and CREST Infrastructure and Application certifications.



Having carried out testing since 2000, Ricoh has one of the longest serving and most experienced penetration testing teams in the industry.



Our testing team has twice won the International Penetration Tester of the Year Award (in 2018 and 2020), competing against other large global cybersecurity providers.



Our services, including red teaming and simulated ransomware attacks are used by some of the largest organisations in the world.

PENETRATION TESTS – WHAT'S INCLUDED



APPLICATION

Finds vulnerabilities and misconfigurations within cloud, SaaS, web and mobile applications



INTERNAL INFRASTRUCTURE

Assess your internal hosts, devices and data to test for compromise, vulnerabilities and misconfigurations



EXTERNAL INFRASTRUCTURE

Assess all internet facing hosts, both cloud and on-premise for vulnerabilities and misconfigurations

- OWASP Top 10
- SQL Injection
- Cross Site Scripting
- Encryption Review
- Authentication Bypass

- Active Directory Compromise
- Wireless Testing
- Firewall Reviews
- Password Cracking
- Vulnerability Scans

- Web Server Compromise
- Email Attacks
- VPN Reviews
- Dark Web Searches
- Password Guessing

OTHER TYPES OF ASSESSMENT



Server and workstation build review



Web server and database build review



Source code review



Red team assessments



Phishing attacks



Simulated ransomware attacks



Cloud health check



Stolen device review



Email, telephone and physical social engineering



Citrix / VDI / RDP assessments



Network traffic analysis



Threat hunting

For more information visit www.ricoh-europe.com/pentesting