BSI Cybersecurity and Information Resilience

Pathway to GDPR Series - Using penetration testing to keep your data safe

BSI Cybersecurity and Information Resilience

Cybersecurity and Information Resilience services enable organizations' to secure information from cyber-threats, strengthening their information governance and business resilience, whilst safeguarding them from any vulnerability in their critical infrastructure.

Consultancy

Training

Research

Technology Solutions

bsi.

End-to-end information security consultancy

Consultancy | **Training** | **Research** | **Technology Solutions**

- **IT Audits/Assessments**
- **Penetration** Testing
- Vulnerability Scanning
- **PCI-DSS** Support
- **Digital forensics**
- Cyber posture **reviews**
- **SDLC**, Architecture
- **Code** Review
- IS **Monitoring**

Tactical

- **IR Strategy Development** (Board Representation)
- **CISO/DPO as a Service** (onsite/virtual)
- **IR Management System** Support + Implementation
- **E-Discovery/Litigation** Support Strategy
- **Critical Infrastructure Security** SCADA/ICS security reviews

Strategic

bsi.

Information resilience training, education, awareness

Consultancy | **Training** | **Research** | **Technology Solutions**

Managerial Security

Technical Security

IT Compliance

eDiscovery and Digital Forensics

bsi.

Research and Development

Consultancy | Training | **Research** | Technology Solutions

Dedicated Research Division

Security and Privacy

Certification and Assurance Frameworks

IOT and Convergence

Big Data

Blockchain

Collaborative EU R&D

SAWSOC

Ecossian

IPACSO

CAMINO

bsi.

Trusted information resilience solution partnerships

Consultancy | **Training** | **Research** | **Technology Solutions**

Vulnerability Management

QUALYS

Information Management

VERITAS

Relativity

Security Awareness

wombat security technologies

Policy Management

netconsent

Managed Security Solutions

ALERT LOGIC
Security. Compliance. Cloud.

EiQ

bsi.

DELL SecureWorks

Cloud Assurance

skyhigh

okta

zscaler

Menlo Security

Vaultive

druva

GDPR Expertise

A range of services to help you achieve compliance

Understanding

- Awareness workshops
- Data asset workflow and mapping
- Gap analysis
- Legal and regulatory assessments
- Data protection risk assessments
- Training and awareness for staff

Implementation

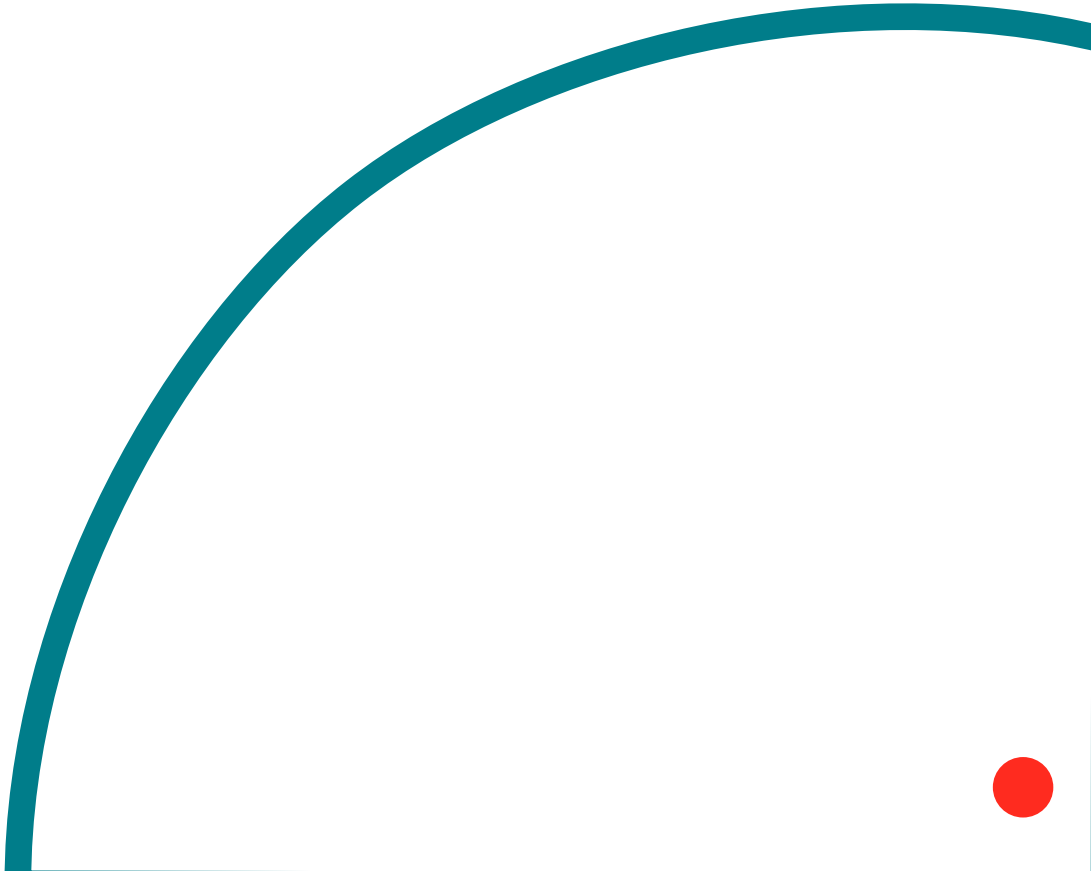
- Outsourced DPO services
- Privacy compliance framework development
- Data protection and privacy implementation support
- Privacy by design support –
- Privacy impact assessments (PIAs) and change management support

Improvement

- Data Protection partner programme service for ad hoc assistance
- Compliance expertise reviews
- Compliance and assurance assessments
  - Privacy compliance audits
  - Internal audits
  - Independent third party audits
  - Preparation for supervisory authority audits
  - Attendance during supervisory authority audits
  - External audits for data transfers outside EU
  - Certifications – e.g. PCI-DSS

bsi.

What is Penetration Testing?



What is Penetration Testing?

- Assessment of technical security by simulating an attack using manual and automated techniques.
- Uses tools and techniques of real attackers.
- Threat actors can be malicious externals or internal users.
- Testing follows robust established methodology.
- Tightly defined scope.
- More focussed than 'Vulnerability Assessments' with greater accuracy.

Business benefits

- Demonstrate compliance with regulators.
- Provide assurance of security to customers, end users and third parties.
- Identify actual vulnerabilities present in systems (rather than just theoretical).
- Identify vulnerabilities present in systems before go-live.
- Help business gain an understanding of the impact of these vulnerabilities.

bsi.

Limitations of Penetration Testing?

- Constrained scope – particularly time.
- Often assesses systems in isolation.
- Provides a snapshot of security at a point of time.
- Does not cover social engineering aspect, such as phishing attacks.
- Often difficult to test the Availability aspect.

bsi.

Webinar Poll 1

Who can/should perform Penetration Testing?

- Penetration testing requires an expert skillset.
- Testers should be part of an industry recognised scheme, such as CREST.
- Staff must be appropriately qualified.
- Ethical and cleared staff.
- Independence is key - if in-house resources, then testers should be 'organisationally' separate from IT or development team.
- Knowledge of systems. 'White/Grey/Black box'

"*Technical compliance review should only be carried out by a competent, authorized persons or under the supervision of such persons.*" *ISO 27002*

bsi.

How frequently should Penetration Testing take place?

- Ultimately, a risk-based decision.
- Also factor in compliance and contractual obligations.
- PCI DSS guidance is:
  - "..at least annually and after any significant infrastructure or application upgrade or modification".
- Seek to retest vulnerabilities following remediation.
- Penetration testing should take place as soon as possible during the project implementation or system development process. The cost of remediation increases significantly the later the project progresses.

bsi.

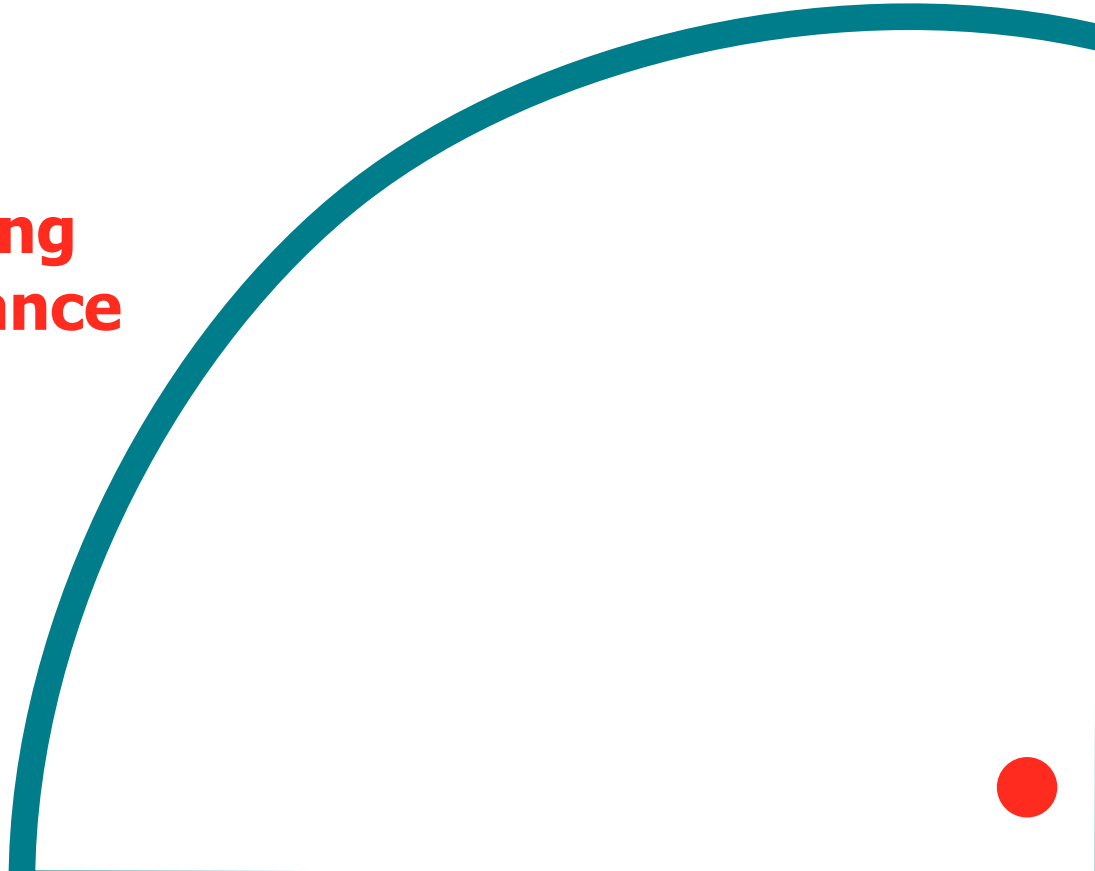
Webinar Poll 2

Getting the most from Penetration Tests

- Ensure you understand what you're commissioning: Vulnerability Scanning is often completely automated and will not weed out false positives.
- Ensure scope is meaningful:
  - Understand your attack surface – who is likely to be targeting your application/system.
  - Perform testing against Production environments wherever possible.
  - The agreed scope is realistic and allows the testers to gain a reasonable view of system security.
  - Sampling can be used where it can be demonstrated that representative samples are being tested.
- Define any specific assurance objectives during the scoping or initiation phase.
- Where possible, allow exploitation of vulnerabilities. Experienced testers will be able to help you make a risk-informed decision.

bsi.

Using Penetration Testing to help achieve Compliance



Compliance

General Data Protection Regulation (GDPR)

- **Integrity and confidentiality** – Article 5(1) – appropriate security
- **Accountability** – Article 5(2) – requires you to demonstrate compliance
- **Data protection by design and by default** – Article 25 – implement suitable technical measures

ISO/IEC 27001/27002

A.12.6.1 - 1 Management of technical vulnerabilities

A.14.1.2 - Securing applications services on public networks.

A18.2.3 - Compliance with information security policies and standards.

Other standards

PCI DSS Req. 11.3

Perform internal/external penetration testing at least annually and after any significant infrastructure or application upgrade or modification.

Gambling Commission

Financial Conduct Authority (FCA)

bsi.

Types of Penetration Test

- Infrastructure penetration testing – servers, endpoints, network infrastructure, firewalls.
- Web Application – such as ecommerce, transactional, HR,

- Mobile Device and Mobile Application
- Device Build Security – servers, endpoints
- Network Device Configurations – assurance of firewall, router, switches.
- Wireless testing
- Telephony and VoIP testing.
- Social Engineering

Webinar Poll 3

Cyber Essentials

Key components:

- Self-Assessment questionnaire
- External Vulnerability scan
- Internal Vulnerability scan and on-site assessment.

5 mitigation strategies:

1. Boundary firewalls and Internet Gateways
2. Secure Configuration
3. Access Control and Privileged Management
4. Malware Protection
5. Patch Management

bsi.

Cyber Red Teaming

- Incorporates Threat Intelligence to provide a realistic test.
- More holistic view of enterprise-wide systems security.
- Less constrained scope: often includes aspects such as Physical Social Engineering and Phishing.
- Scenario-based testing agreed at scoping phase.
- Helps organisations assess their Response/Detection capabilities
- Engagements typically last several weeks
- CREST Simulated Attack and Response (STAR) standard.
- BSI is a CREST accredited STAR provider.

Webinar Poll 4

Ransomware

Questions?

...making excellence a habit.™