Untrained employees - the weakest link in your cybersecurity defence

Richard Lambe

Senior Security Awareness Consultant

Through the passion and expertise of our people, BSI embeds excellence in organizations across the globe to improve business performance and resilience.

Cybersecurity and Information Resilience – what we do

We enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

bsi.

What do we do?

Cybersecurity

Penetration Testing
Vulnerability Management
Cloud Security
Lab Testing (inc. IoT)
Ethical Hacking Training (CEH)

Risk Management

ISO27k development/implementation
PCI DSS
GDPR Compliance Services
Information Compliance Training
Security Management Training (CISM)

Data Management / Data Protection

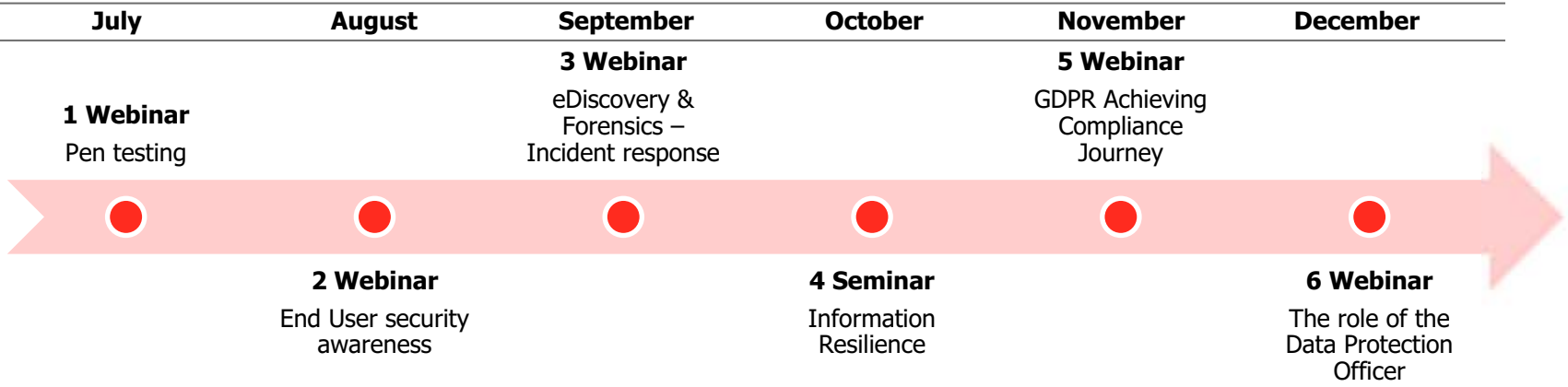
GDPR Professional Services
eDiscovery / eDisclosure
Digital Forensics & Incident Investigation
Information Lifecycle Management + Governance
Privacy Management Training (CIPP/E, CIPM, CIPT)

End User Security Awareness

SaaS Solutions (Wombat)
Phishing and Awareness Training
Social Engineering
Simulation Testing

bsi.

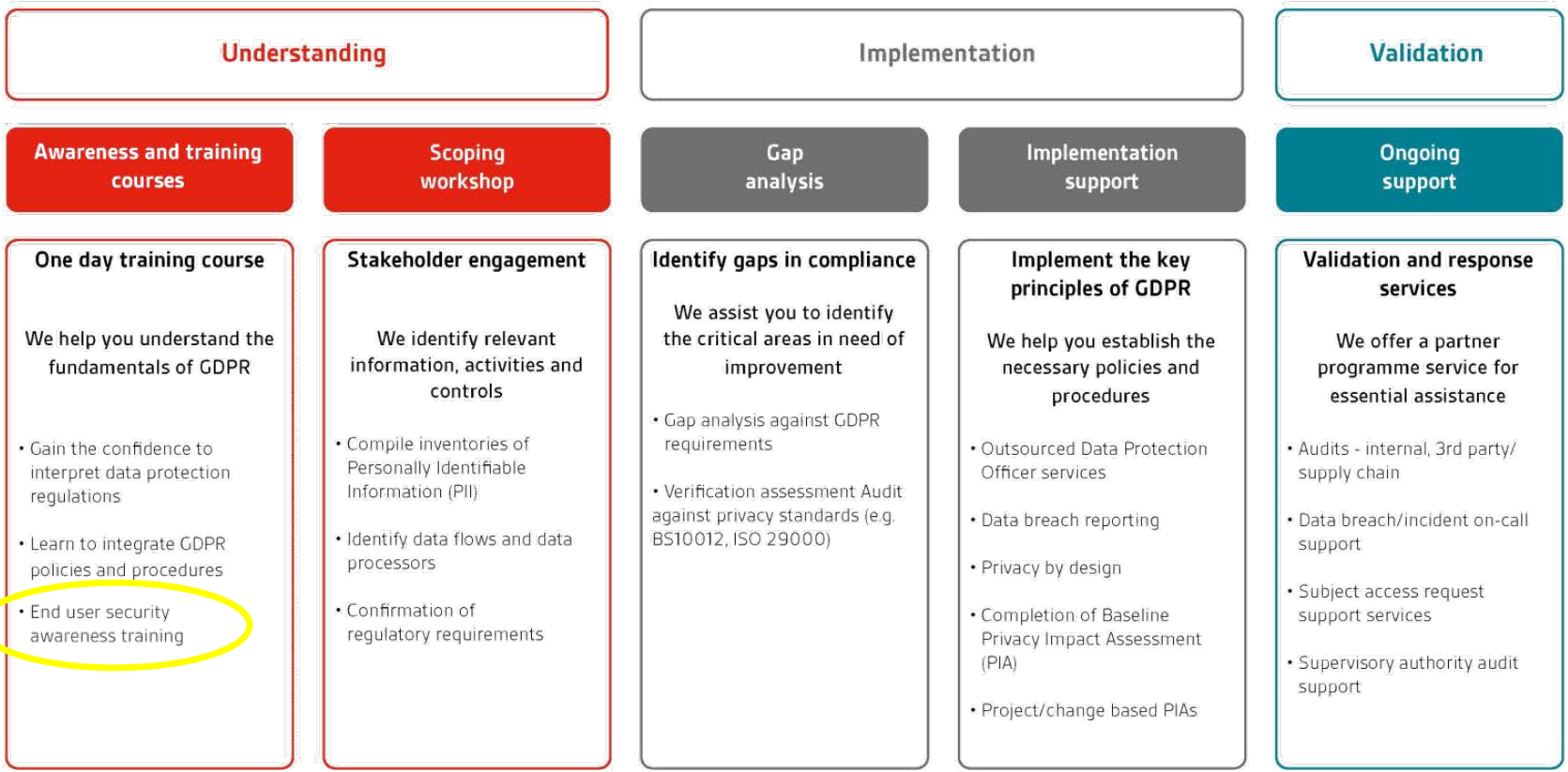
Path to GDPR – Cybersecurity and Information Resilience Services



Webinar Series:

1. **Penetration Testing (Jul17) –** ensuring an organization's customer and prospect data is secure
2. **End User Security Awareness (Aug17)** – Untrained employees - the weakest link in your cybersecurity defence
3. **Incident Response (Sept17) –** You have 72 hours to respond after a breach... was personal data compromised?
4. **Information Resilience Series Event (Oct17)** – Manchester 17th October 2017
5. **GDPR Achieving Compliance Journey (Nov17)** – a step-by-step methodology for achieving compliance
6. **GDPR – the role of the Data Protection Commissioner (Dec17)** – Is your organization's DPO ready?

bsi.


Understanding
Implementation
Validation
Awareness and training courses
Scoping workshop
Gap analysis
Implementation support
Ongoing support
One day training course
We help you understand the fundamentals of GDPR
• Gain the confidence to interpret data protection regulations
• Learn to integrate GDPR policies and procedures
• End user security awareness training
Stakeholder engagement
We identify relevant information, activities and controls
• Compile inventories of Personally Identifiable Information (PII)
• Identify data flows and data processors
• Confirmation of regulatory requirements
Identify gaps in compliance
We assist you to identify the critical areas in need of improvement
• Gap analysis against GDPR requirements
• Verification assessment Audit against privacy standards (e.g. BS10012, ISO 29000)
Implement the key principles of GDPR
We help you establish the necessary policies and procedures
• Outsourced Data Protection Officer services
• Data breach reporting
• Privacy by design
• Completion of Baseline Privacy Impact Assessment (PIA)
• Project/change based PIAs
Validation and response services
We offer a partner programme service for essential assistance
• Audits - internal, 3rd party/ supply chain
• Data breach/incident on-call support
• Subject access request support services
• Supervisory authority audit support

General Data Protection Regulation in 1 Minute

- aims to **protect** the personal data of EU citizens
- puts individuals back in **control** of their personal data
- applies to all EU member states, any organization who operates within the EU market, or who holds information on EU data subjects
- requirement to **report** a data breach to the Data Protection Commissioner, within 72 hours of becoming aware of any breach
- **fines** of up to €20 million or up to 4% of annual worldwide turnover for non-compliance
- comes into force on the **25th May 2018**
- Data Protection Officer (DPO) appointment **mandatory**
- No opt out for UK with **Brexit**

Training & the GDPR

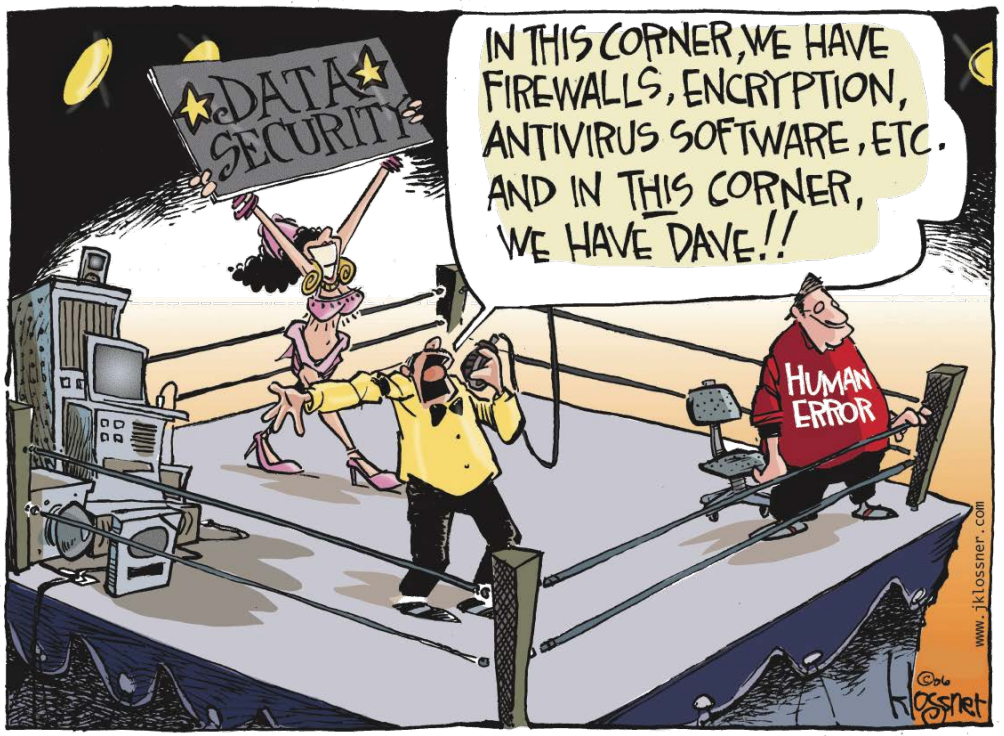
Article 39 – Tasks of the data protection officer

The data protection officer shall have at least the following tasks;

(b) to monitor compliance… including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations

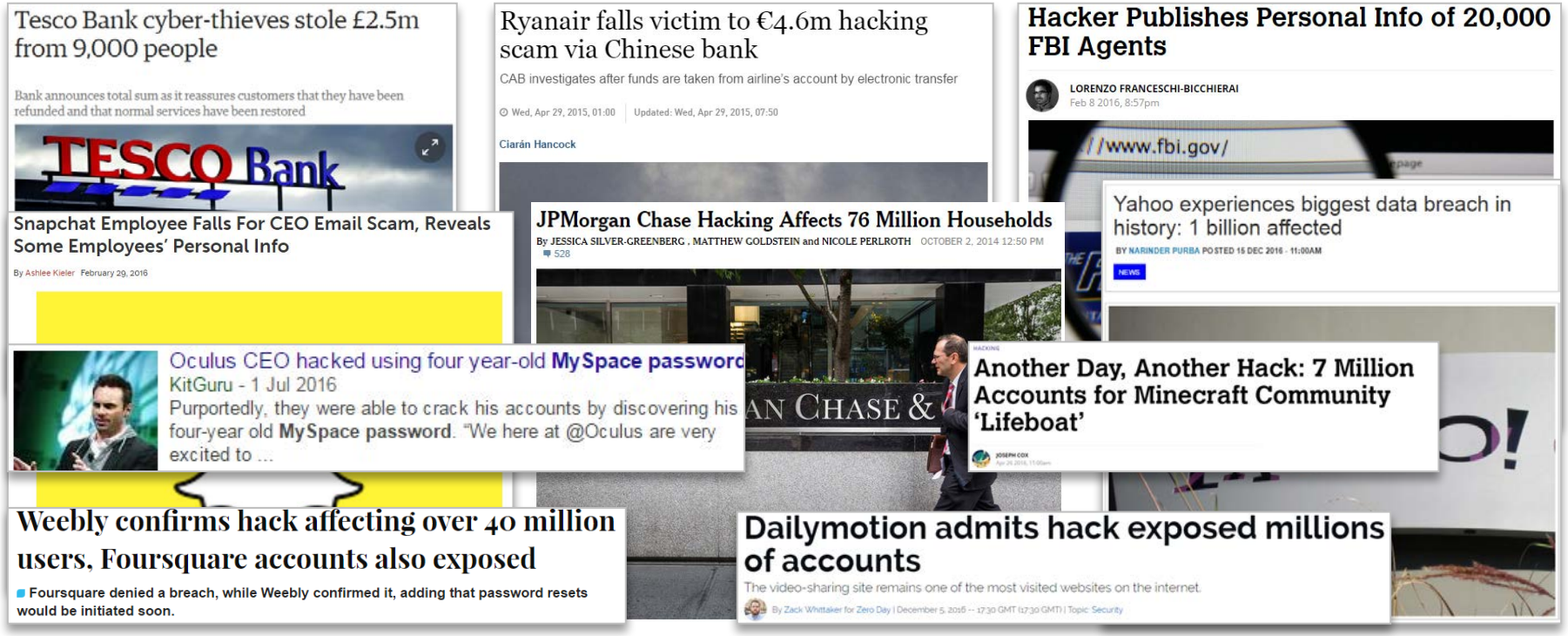
Image from European Data Protection Supervisor
https://edps.europa.eu/data-protection/our-work/subjects/data-protection-officer_en

GDPR & the People Factor

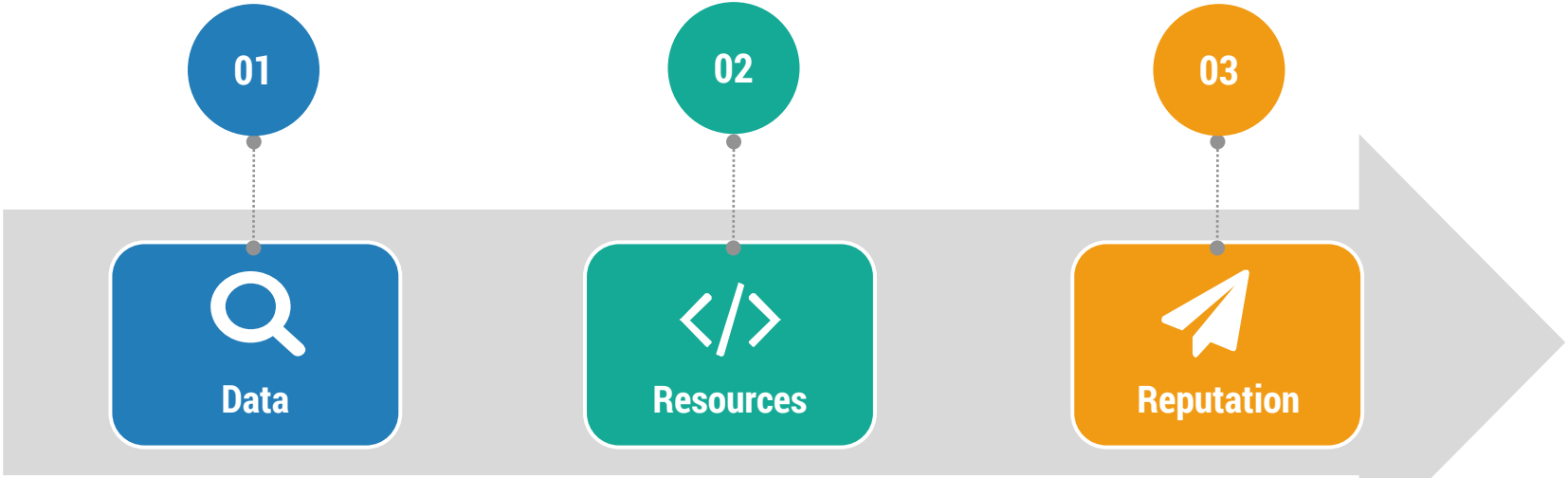


Poll #1

In the news…



You need to protect your…



This may include client information, intellectual property or your staff's personal data.

Your resources may include finances, files, computers, servers, building facilities or people.

Your brand is only as good as your reputation. Ensuring your clients have confidence in you is extremely important.

Why End Users Matter

90% of employees admit to violating policies designed to prevent security incidents.[1]

60% of senior IT executives across 200 medium to large UK organizations regard staff as the biggest threat to GDPR adherence.[2]

87% of IT professionals said that careless employees represented a greater threat to security than cybercriminals.[3]

1: 2017 Cyber Incident & Breach Response Guide
2: Bluesource GDPR Survey 2017
3: Checkpoint Study: The Impact of Mobile Devices on Information Security: A Survey of IT and Security Professionals

World's most popular password?

123456

Used in 17% of hacked accounts in 2016

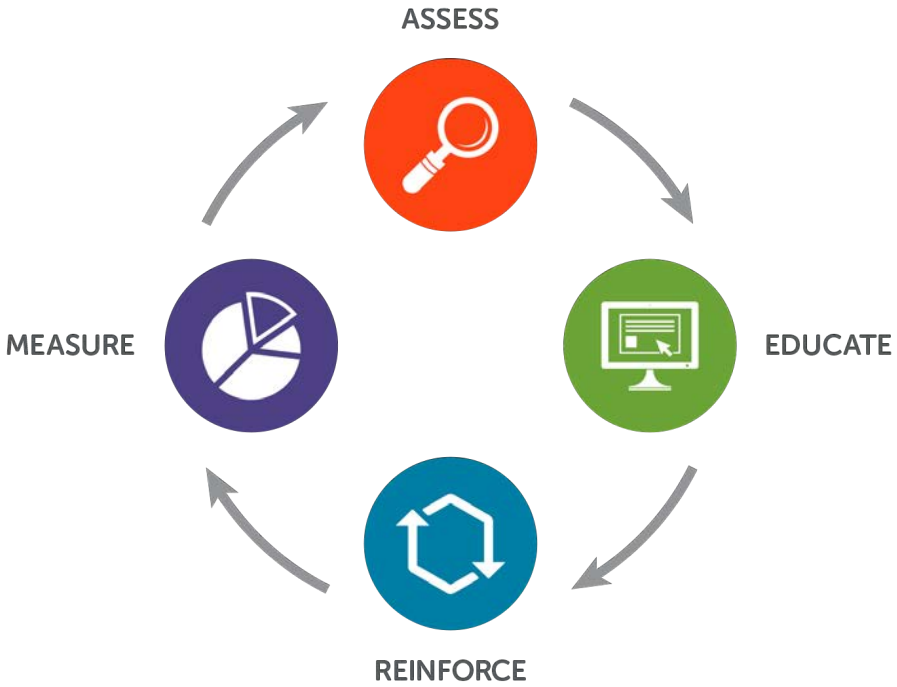
Source: http://www.theregister.co.uk/2017/01/16/123456_is_still_the_worlds_most_popular_password/

Create a Culture of Security Awareness

Complete, effective, security awareness program

- End user training & assessments
- Lasting behaviour change
- Reduce risk to cyber threats
- Cloud or LMS based training

Continuous Training Methodology



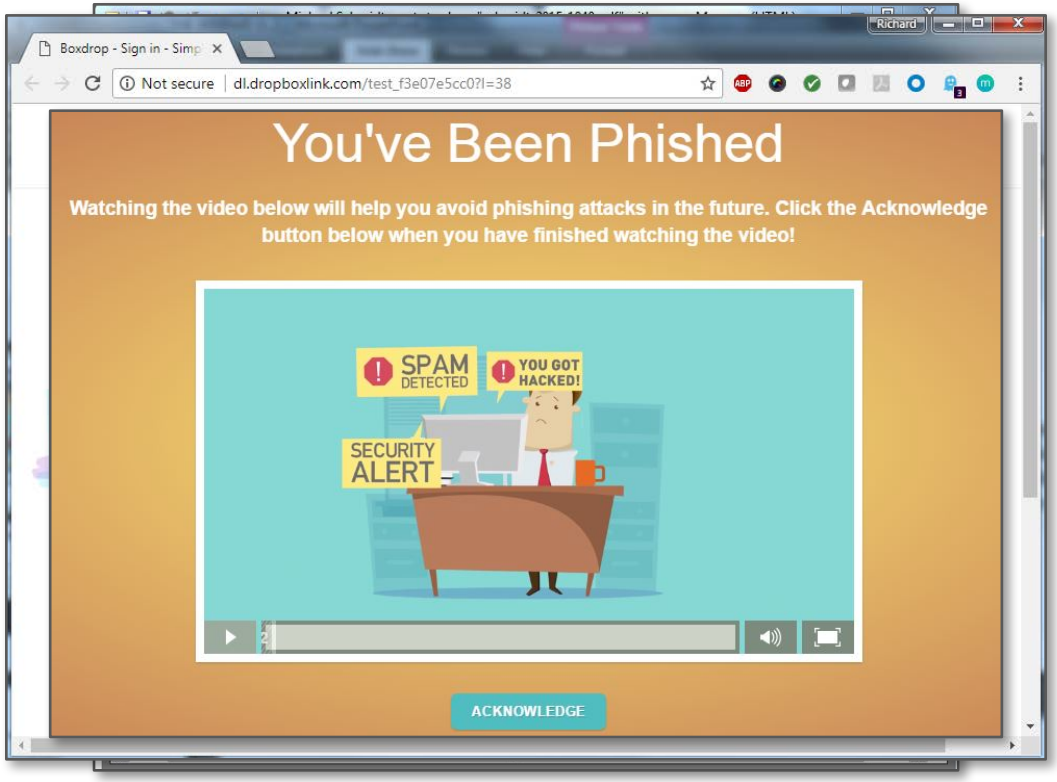
Poll #2

Assess

Knowledge assessments
Simulated attacks

Detect “human” vulnerabilities in the organization

Assess: Simulated Phishing Emails



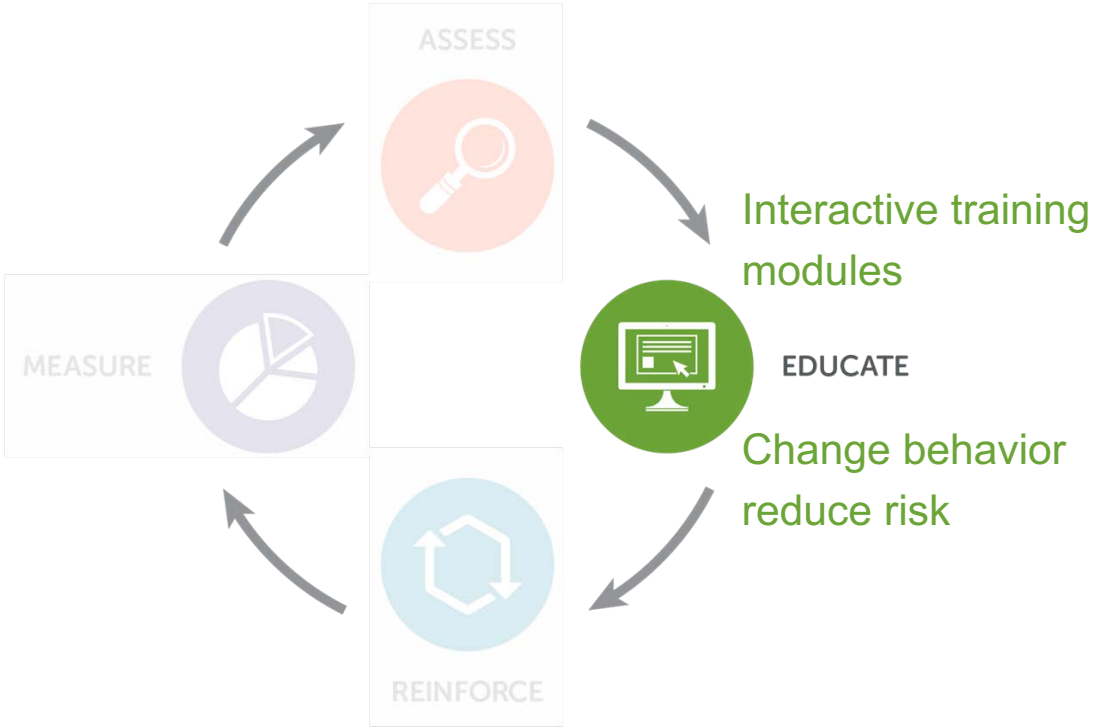
- Auto-enrolment
- Drip feed emails
- Anonymise Results
- Ransomware Prep
- CEO Fraud

Assess: Scenario Based Quizzes

- User Defined Questions
- Auto-enrol to training
- Real world scenarios
- Feedback on answers

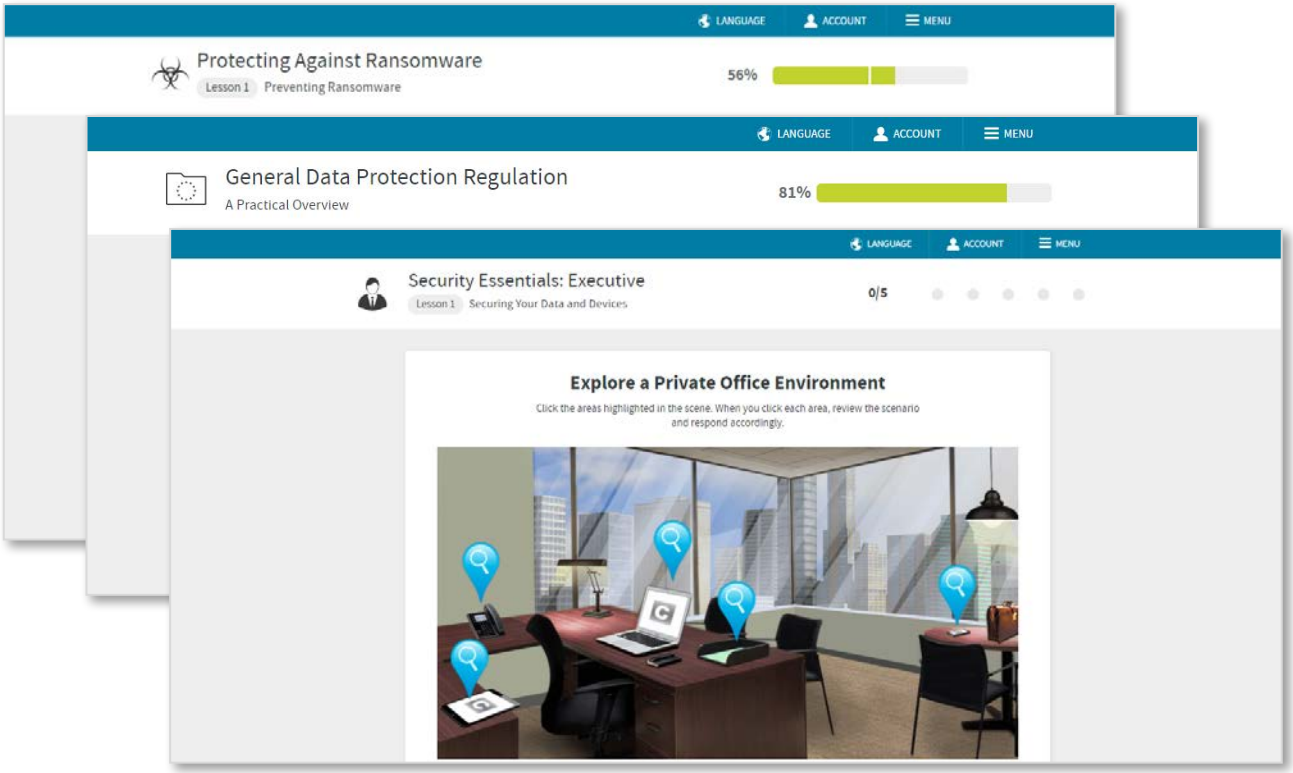
Poll #3

Educate



Educate: Engage Employees Through Interactive Training

- Interactive & Engaging
- Max 10 minutes
- Real World Examples
- Learn by Doing
- Stories & Scenarios
- Mobile Responsive



Educate: Executive Level Training

Interactive face-to-face sessions

Up to 4 hours ideally after group meeting

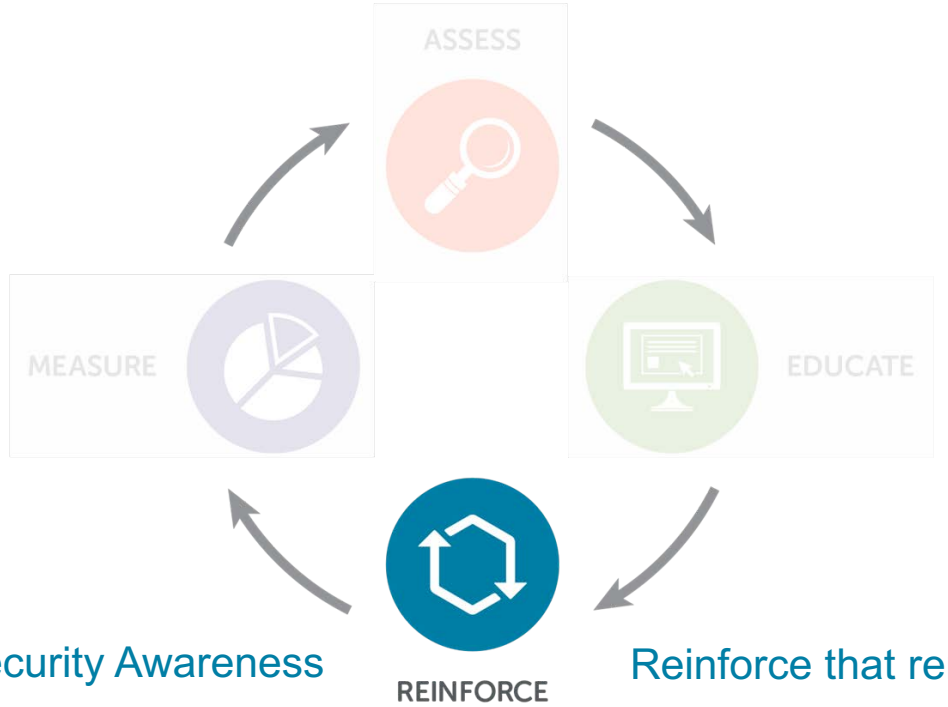
Stakeholders, Risk Owners, Non-Technical Senior Management

Understand their roles to play in GDPR

Increase awareness in such areas as;

- CEO fraud
- Business email compromise
- Whale phishing

Reinforce



Security Awareness Materials

Reinforce that remediation on an ongoing basis

Reinforce: Posters, Screensavers & Videos

- Remind, Reinforce, Retain, Respond
- Educational messages imagery & video
- Emphasize best practices
- Encourage good behaviour

Reinforce: Suspected Phish Reporting

- One-click phishing report plugin
- Simplifies process of reporting phishing emails
- Reduces helpdesk calls
- Positive reinforcement by thanking users

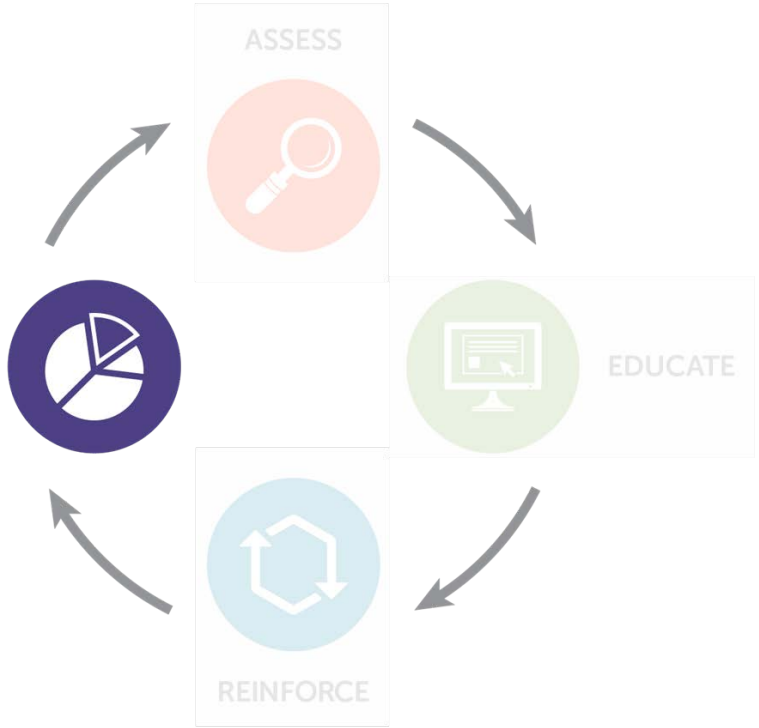
PhishAlarm™

Measure

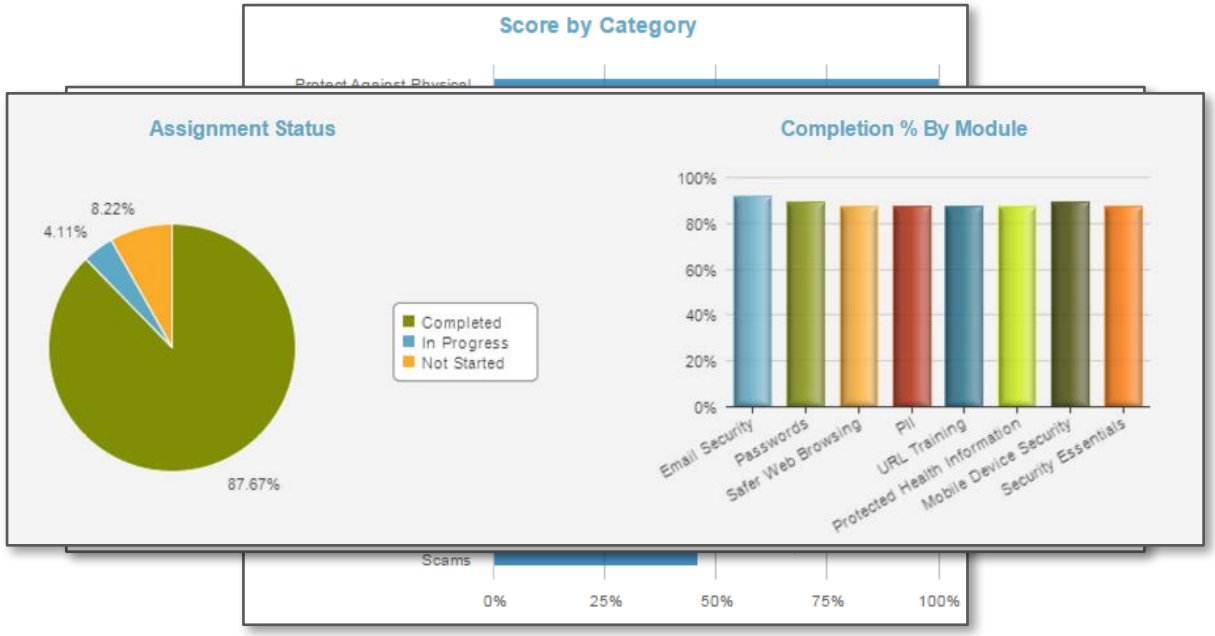
Detailed reporting capabilities

MEASURE

Benchmark, track results, measure risk



Measure: Identify weaknesses, plan campaigns



- Powerful Analytics
- Compare Results
- Export Results for Compliance
- Plan Future Training
- Clearly show improvement over time

Results

Compliance & Law

EU General Data Protection Regulation (GDPR)
Each individual country's implementation of this directive will involve a requirement to provide security awareness training

ISO 27001
"All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training"

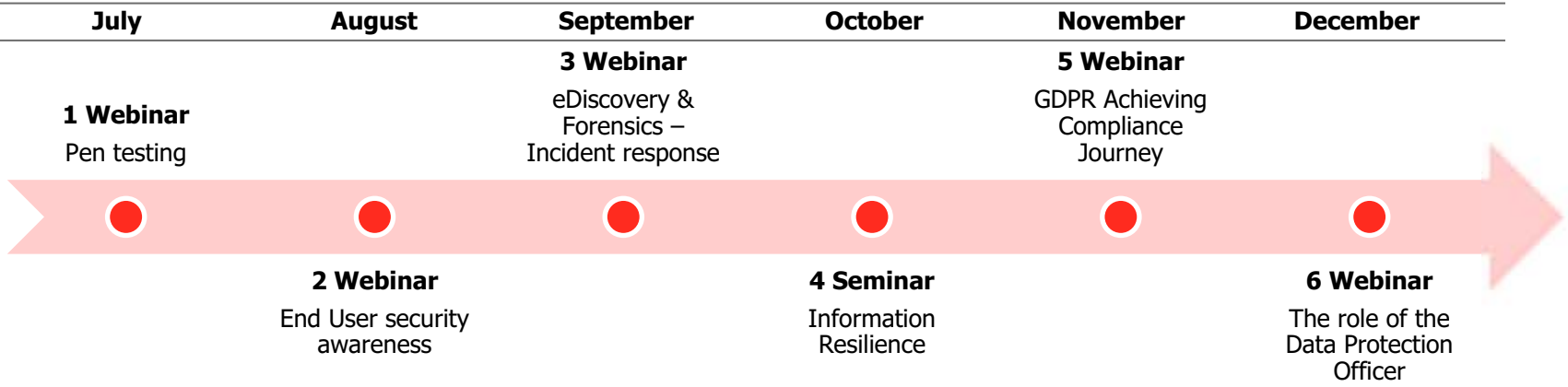
PCI-DSS
"In order for an organization to comply with PCI DSS Requirement 12.6, a formal security awareness program must be in place."

To summarize

1. Your employees – strongest asset/weakest link
2. The GDPR is here to help, and so are your employees
3. Stay out of the news – roll out a comprehensive security awareness program
4. The human firewall – continuous training methodology
5. Review current internal measures in place – are these good enough to avoid GDPR non-compliance?

"Depending on which study you read, anywhere between 60% and 95% of all security breaches involve human error."
Forbes.com, November 2016

Path to GDPR – Cybersecurity and Information Resilience Services



Webinar Series:

1. **Penetration Testing (Jul17) –** ensuring an organization's customer and prospect data is secure
2. **End User Security Awareness (Aug17)** – Untrained employees - the weakest link in your cybersecurity defence
3. **Incident Response (Sept17) –** You have 72 hours to respond after a breach... was personal data compromised?
4. **Information Resilience Series Event (Oct17)** – Manchester 17th October 2017
5. **GDPR Achieving Compliance Journey (Nov17)** – a step-by-step methodology for achieving compliance
6. **GDPR – the role of the Data Protection Commissioner (Dec17)** – Is your organization's DPO ready?

bsi.

Poll #4

Get in touch

UK – End User Security Awareness

Phone: 00 44 345 222 1711

Email: cyber@bsigroup.com

Global – End User Security Awareness

Phone: 00 353 1 210 1711

Email: cyber.ie@bsigroup.com