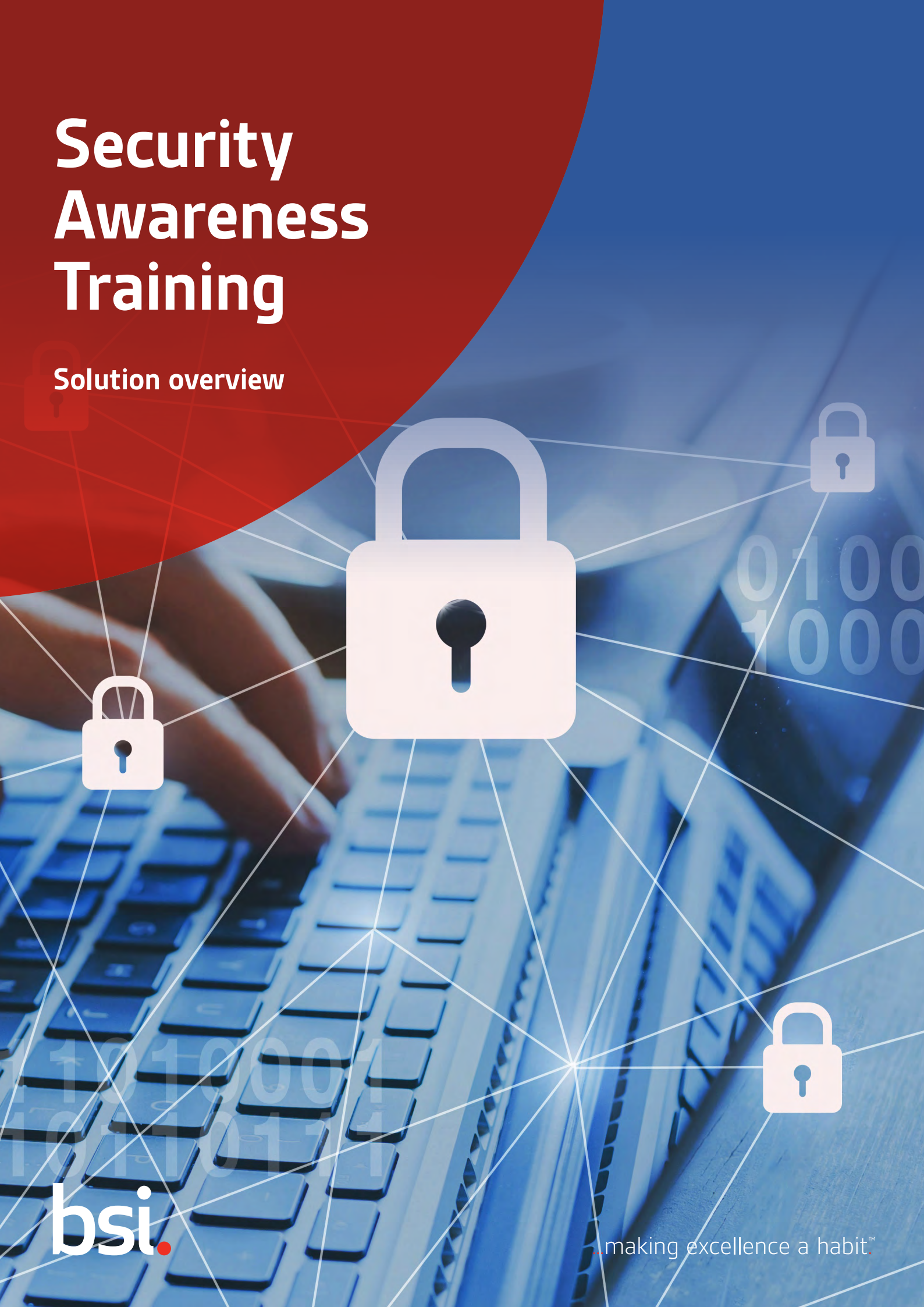
Security Awareness Training

Solution overview



bsi.

making excellence a habit.™

Solution overview

Proofpoint Security Awareness Training

Proofpoint Security Awareness Training (formerly Wombat Security) helps you deliver the right training to the right people at the right time, turning your end users into a strong last line of defense to identify cyberattacks and protect your organization.

Key benefits

- Change users' behaviour to reduce risks from phishing and other cyberattacks
- Prioritise and improve incident response
- Provide consistent training across the globe with multi-language support
- Track results and progress with real-time reporting
- Reduce successful phishing attacks and malware infections by 90%

With more than 90% of cyber attacks starting with an email, wary end users are critical to protecting your people and your data. While technologies that detect and block malicious emails are part of the solution, you can also reduce the likelihood of successful attacks such as phishing or ransomware through effective, broad-based security awareness training.

Protect your organization with phishing simulations

ThreatSim® Phishing Simulations help you understand your organization's susceptibility to a variety of phishing and spear-phishing attacks. With thousands of different phishing templates across 13 categories, you can evaluate users on multiple threat types, including:

- Malicious attachments
- Embedded links
- Requests for personal data

We add new templates every month. Our Dynamic Threat Simulation phishing templates are drawn from Proofpoint threat intelligence; others reflect customer requests and seasonal topics.

Users who fall for a simulated attack receive practical 'just-in-time' teaching. They learn the purpose of the exercise, the dangers of real-world attacks, and how to avoid future traps. You can also help your most vulnerable users by automatically assigning interactive training to anyone who falls for a phishing simulation.

Access vulnerabilities with our knowledge assessment tool

CyberStrength® is a powerful web-based knowledge assessment tool that identifies your employees' potential vulnerabilities – without having to run a simulated phishing attack. After establishing a baseline measurement of your employees' understanding, periodic reassessments allow you to track progress and target areas of concern.

We offer a library of more than 200 questions, across a range of critical cybersecurity topics. You can also create custom questions to gauge knowledge of your organization's policies and procedures. With CyberStrength, you can identify where you are susceptible – from an organizational level down to the individual.

Educate employees with engaging, actionable training content

Our growing, continuously updated content library offers interactive training modules, videos, posters, and images in 35+ languages, with consistent, actionable messaging suitable for global organizations. Based on proven learning science principles, our customizable education content covers a broad range of security risks, from phishing attacks to insider threats.

Our interactive training modules are available on demand and are mobile-responsive, so your users can take our training anytime, anywhere, on any connected device, maximizing efficiency and convenience. The modules take an average of just 5 to 15 minutes to complete – minimizing disruption to daily work routines – and conform to the US Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.

We also make it easy to alert your users to the most relevant phishing attacks and lures through our Attack Spotlight series – brief, timely content that teaches how to spot a current threat and avoid becoming a victim.

Reduce risks with our automated alert system

PhishAlarm® is an email client add-in that allows your people to report suspicious messages with a single mouse click. Users who report an email get instant positive reinforcement in the form of a "thank you" pop-up message or email. Using PhishAlarm Analyzer, reported messages are automatically analyzed and enriched using multiple Proofpoint Threat Intelligence and reputation systems. And they are dispositioned as malicious, suspicious, bulk or spam.

With our CLEAR (Closed-Loop Email Analysis and Response) solution, reported messages are sent to TRAP (Threat Response Auto-Pull). In TRAP, the different classifications of messages can be automatically quarantined or alerted to incident response teams for investigation. With this solution, active attacks can be stopped in minutes with the help of trained end users.

Analyze results with full-featured reporting

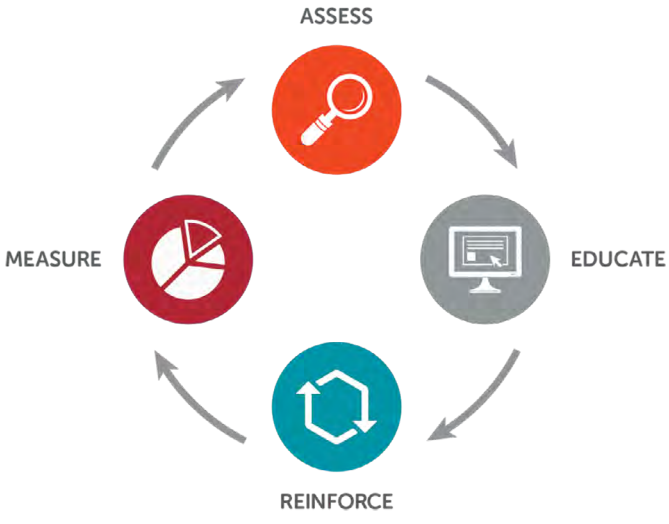
Our reporting capabilities provide the granular and high-level visibility you need into your employees' interactions with assessments, simulated attacks, and training assignments. We offer responsive, easy-to-read reporting with a modern UI, providing more than just completion data so that you can evaluate progress, gauge ROI, and benchmark, track, and trend user knowledge. You can use our dashboards to easily filter data, compare assessments, quickly add and remove measures, and more.

You can also download and export data to share business intelligence with other stakeholders, perform more detailed analysis, and evaluate metrics alongside other security events. Our automated reporting feature streamlines the export process, allowing you to schedule automatic delivery of reports at regular intervals to yourself and designated stakeholders within your organization.

About our continuous training methodology

Industry research has shown that once-a-year classroom training is not effective in the battle against cyberattacks. Our unique Continuous Training Methodology is a cyclical approach that teaches users about best practices and how to employ them when facing security threats.

A continuous cycle of assessment, education, reinforcement, and measurement maximizes learning and lengthens retention. Our methodology sits in strong contrast to a 'one and done' approach, giving you the flexibility to evolve your program over time, identify areas of susceptibility, and deliver targeted training when and where it's most needed.



Interactive training modules

A unique, effective approach to security awareness training

Proofpoint Security Awareness Training provides training based on research-proven Learning Science Principles that help elevate the effectiveness of cybersecurity education. Our learning science principles have earned praise from customers and end users alike, and are designed to help you deliver the right training to the right people at the right time.

- Lessons are brief and focused. Each module takes only 5 to 15 minutes to complete, on average.
- Mobile-responsive design allows users to take training anytime, anywhere, on any connected device.
- Modules conform to the U.S. Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.
- Modules are available in 35+ languages. Professionally translated and localized content delivers high-quality, engaging training for employees around the globe.
- Flexible, on-demand format minimizes disruption to daily work routines. Continuous updates ensure that training is relevant and up-to-date.
- Gamification techniques and interactivity keep end users engaged. Employees set the pace and receive feedback throughout.

Securing Your Email – Fundamental Series

Introduction to Phishing
Teaches users how to recognize email traps and avoid phishing scams.

Avoiding Dangerous Attachments
Focuses on identifying and avoiding dangerous email attachments.

Avoiding Dangerous Links
Explains common email traps and how to avoid dangerous links.

Data Entry Phishing
Teaches users how to identify and avoid scams that request personal or sensitive data.

Password Protection Series

Beyond Passwords
Explains how to use PINs and passphrases to secure devices and accounts.

Multi-factor Authentication (MFA)
Focuses on adding an extra level of security to accounts using multi-factor authentication.

Password Management
Explores best practices and strategies for safely managing passwords.

Password Policy
Teaches users how to create passwords compliant with your company's policy.

Securing your Email – Advanced Series

Email Protection Tools
Teaches users how to protect themselves from phishing scams in combination with email defense tools.

Email Security on Mobile Devices
Explores how to identify and avoid phishing emails on mobile devices.

Spear Phishing Threats
Trains users to recognize and avoid targeted phishing attacks.

Insider Threat Series

Insider Threat Overview
Introduces the concept of insider threats and best practices for protecting against them.

Malicious Insider Threat
Presents users with real-world examples where they can discover actions that help mitigate malicious threats.

Unintentional Insider Threat
Walks users through scenarios that highlight employee actions that cause unintended threats.

Personally Identifiable Information (PII) Series

PII in Action
Presents users with various scenarios to learn how different decisions affect our ability to safeguard PII.

PII Fundamentals
Teaches users how to protect confidential information about themselves, your organization and your customers.

Preventing Compromise Series

Identifying Compromised Accounts
Identify how and why attackers compromise accounts. Learn best practices to avoid the scams associated with a compromised account, such as email fraud.

Mitigating Compromised Devices
Identify how and why attackers compromise devices. Learn best practices to avoid a compromise or a scam associated with a compromise.

Other Training

Data Protection and Destruction
Teaches employees how to use portable storage safely and properly dispose of sensitive data.

Email Security
Teaches users how to identify phishing emails, dangerous attachments and other email scams.

GDPR Overview
Introduces users to protecting personal data under the General Data Protection Regulation.

GDPR in Action
Trains users to apply concepts outlined in the GDPR to everyday situations and decisions.

Mobile App Security
Teaches users how to judge the safety of mobile apps.

Mobile Device Security
Explains physical and technical safeguards for protecting devices and data.

Physical Security
Teaches users how to keep people, areas and assets more secure.

Protected Health Information (PHI)
Teaches employees why and how they should safeguard Protected Health Information.

Protecting Against Ransomware
Teaches users how to recognize and prevent ransomware attacks.

Safe Social Networking
Shows users how to use social networks safely and responsibly.

Safer Web Browsing
Focuses on staying safe on the internet by avoiding risky behavior and common traps.

Security Beyond the Office
Shows users how to avoid common security mistakes while working at home or on the road.

Security Essentials
Explores security issues commonly encountered in daily business and personal activities.

Security Essentials – Executive
Teaches users how to recognize and avoid threats senior managers encounter at work and at home.

Social Engineering
Teaches users how to recognize and avoid social engineering scams.

Travel Security
Explores how to keep data safe when working in airports, hotels and other public spaces.

Understanding PCI DSS
Shows users how to recognize warning signs and improve security of credit card data.

URL Training
Explains how to spot fraudulent URLs.

USB Device Safety
Teaches users to protect themselves, data and systems when using USB devices.

Workplace Security in Action
This scenario-based module reinforces key components of office security and covers topics such as social engineering, insider threats and shoulder surfing.

Packages summary

Proofpoint Security Awareness Training provides an added layer of security by testing and educating employees about the latest threat trends. From Proofpoint, a Gartner MQ leader, these unique tools and methodology helps you reduce the number of successful phishing attacks and malware infections.

	Anti-phishing	Enterprise
Description	Teach end users to defend against just phishing attacks. Receive the most comprehensive and effective library of anti-phishing training available.	Provides all of the products and features necessary to fully implement our Continuous Training Methodology, which produces the most effective results for changing users' behavior.
CyberStrength® Knowledge Assessments		✓
ThreatSim® Simulated Phishing Attacks	✓	✓
ThreatSim® USB Simulation		✓
PhishAlarm® Email Reporting Button	✓	✓
PhishAlarm Analyzer Threat Prioritization	✓	✓
End User Sync with Active Directory (AD)	✓	✓

	Anti-Phishing	Enterprise
Interactive Training Modules	**Receive 8** • Securing your email – fundamentals • Securing your email – advanced • Email security • URL training • Social engineering • Protecting against ransomware • Anti-phishing Phil™ • Anti-phishing Phyllis	**Receive all**
LMS (SCORM) Installation	✓	✓
Education Materials	Add-on	✓
Awareness Video Campaigns	Add-on	✓

Additional features and benefits

Reports and analytics

- Automated reporting for delivering reports to key stakeholders
- Dynamically filter data using dozens of parameters
- Export to XLS and CSV
- Benchmarking against other Proofpoint customers including industry-specific data

Multinational support

- Assessments and training translated and localized into 35+ languages
- Support for international time zones
- Regional data storage and data privacy features
- Regionally-specific domains, names, and references, plus more

End-user accessibility

- Single sign-on to our Security Education Platform
- Mobile accessibility for Interactive Training Modules*
- 508 and WCAG Compliance
- 2.0 AA

Administration and security

- Unlimited use of assessments, training, and reporting for licensed end users
- Two-factor authentication for administrators
- Limit password reuse and lock- out after failed login attempts
- Customize password policy of administrators in our Security Education Platform

Support and services

- Award-winning support via email, phone, and live chat
- Online community with knowledge base, ideas, discussions, and more
- Customer Engagement Manager assigned to your account
- Access to extensive best-practices documentation

Technical certification

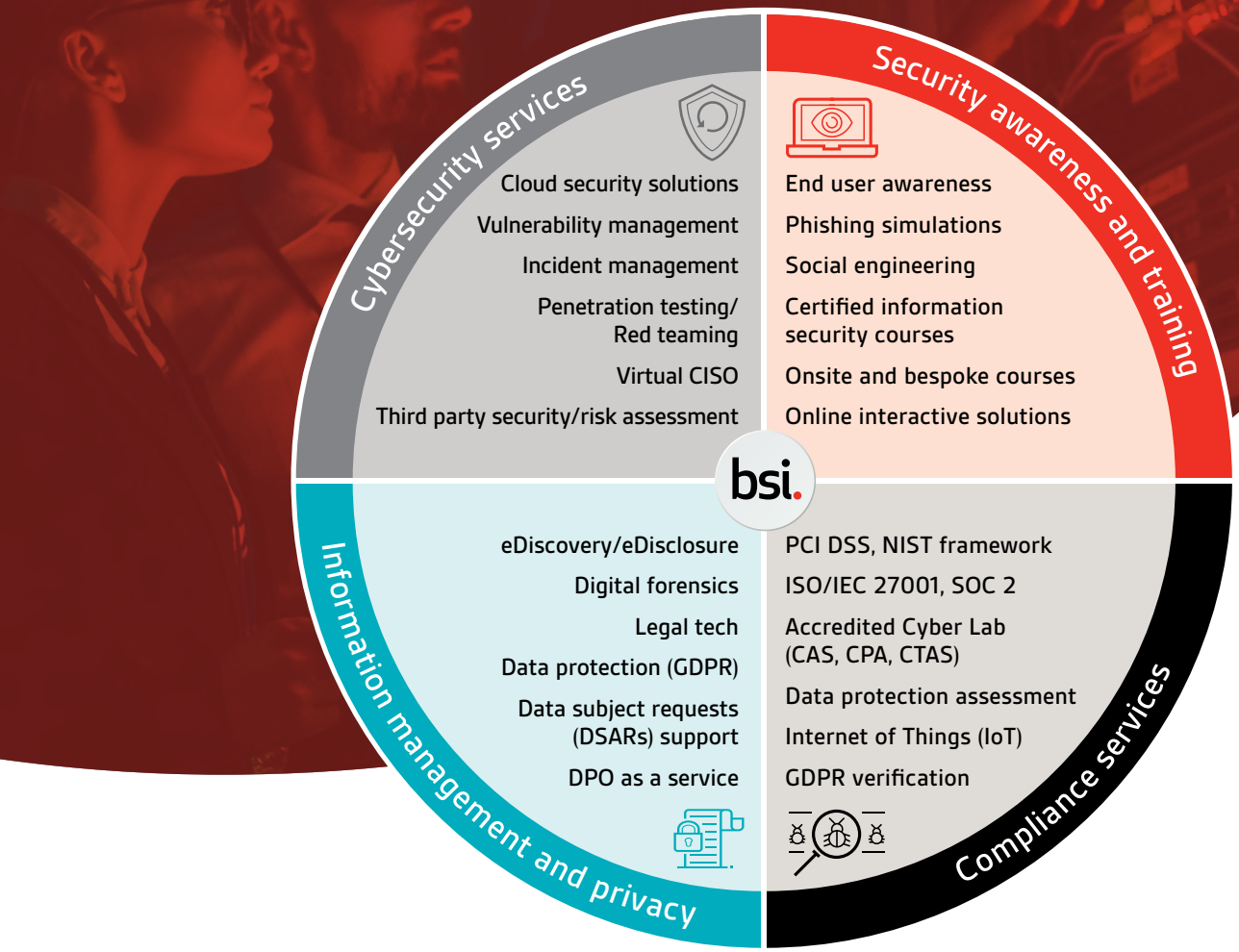
- Annual independent third-party Data Privacy Assessment by TRUSTe
- Self-certified with EU-US Privacy Shield and the Swiss-US Privacy Shield Frameworks
- Cloud Security Alliance STAR Self-Assessment
- Okta Integration Partner for single sign-on
- FedRamp Moderate Certification "In Process"

* All training modules are mobile responsive except URL Training, Mobile App Security, Email Security, Anti-Phishing Phil, and Anti-Phishing Phyllis.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



Our expertise is accredited by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™ · CYBER ESSENTIALS · CREST STAR · CHECK IT Health Check Service

bsi.

Find out more

UK
Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com/cyber-uk

IE/International
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

US
Call: +1 800 862 4977
Email: cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-us