HOLISTICYBER | SOLUTION BRIEF
DEFEND WHAT MATTERS

Cyber Training & Awareness Testing

Creating a Cyber Aware Workforce

What is the Cyber Training & Awareness Testing Service?

Cyber Training & Awareness Testing is a tailored service designed to create a cyber-aware, resilient workforce and culture. The service includes training employees (end-users) to be aware of the many cyber threats in their environments and how to avoid deceptions and pitfalls from cyber offenders.

Additionally, the service offers a security training program for technical/IT team members. Orchestrated by nation-state grade domain experts, the service helps IT, Security, and Compliance leaders build a cyber-aware culture where employees recognize and avoid falling victim to cyberattacks.

With content incorporating threat intelligence insights, the service arms employees with the latest knowledge, guidance, and tips to make smarter choices when confronted by cyber-attacks and other risks to the organization.

How does Cyber Training & Awareness Testing work?

Non-technical employees - we create a path of actionable and customized training on the importance of security in their language to foster a security-focused culture and a robust first line of defense. Employee training includes, but is not limited to:

- Responsibility for company data
- Document management and notification procedures
- Passwords
- Unauthorized software
- Internet use
- Email
- Social engineering and phishing
- Social media policy
- Mobile devices
- Protecting computer resources

IT teams / technical employees – cyber defense experts walk through up-and-coming threats from strategic and practical perspectives to keep IT teams up to date on the newest threats and techniques to defend against them. For example, our experts mimic real phishing scenarios and other types of attempts specific to the industry. Training includes, but is not limited to:

WHAT SHOULD YOU EXPECT?

- **Training employees to recognize and report on potential security threats whether in an email, online or in a physical setting.**
- **Prevent the impact of breaches caused by employee errors and poor judgment.**
- **Up-to-date training based on the newest emerging threats and prevention techniques.**
- **Comprehensive long and short-term training plan.**
- **Training programs for both technical and non-technical employees.**
- **Success benchmarks specific to the organization.**
- **Continuous phishing simulations and testing.**
- **Satisfy requirements for security and awareness training across major frameworks including PCI DSS, GDPR, CCPA, and other frameworks.**
- **Reduce the costs and strain on security and IT in managing infections and removing malware.**
- **Testing scenarios based on known attacker behavior, tactics, and techniques.**

- Review of current training plan
- Cultivating a plan that suits the organization
- Learning the attackers' perspective
- New threats overview, including tactics, techniques, and procedures
- Avoiding repetitive problems by establishing continuous training plans and retesting.
- New technology training
- New defense techniques

How can enterprises keep up with today's cyber threats? By getting ahead of them.

With the growing number of cyber threats facing organizations and the overwhelming number of tools to combat them, IT and security teams typically suffer a considerable skills gap. Depending on the organization's size, anywhere from 15-130 security tools are being used at any given time. New threats are emerging while nation-states are targeting the private sector. It is challenging to keep up with all of this, but with the proper training, protecting company data and assets becomes more approachable.

Additionally, employees must be aware of their responsibilities and accountabilities when using computers and smart devices on the business networks and while working from home. New hire training and regularly scheduled refresher training sessions should be established to instill the data security culture of the organization.

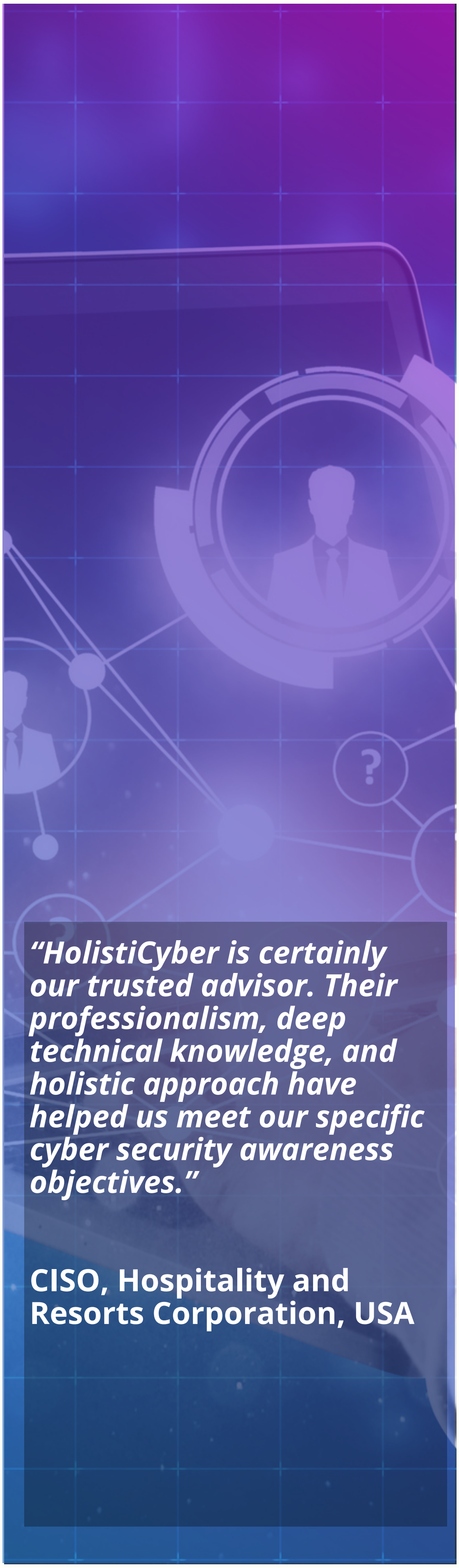
The phishing problem.

Part of security awareness training must focus on phishing as it is responsible for the bulk of breaches. Users get hoodwinked into clicking on a malicious attachment or URL, which inadvertently provides cyber offenders with a convenient entry point to the corporate network.

Cybercriminals often create fake emails, posing as trusted vendors, government agencies, or a person within the company, a deceptive practice known as spoofing. Attackers usually fashion subject lines designed to gain attention and increase the chances that someone will click on a link. It takes discipline to think before clicking on an urgent link from the CEO. Thus the goal of training is to educate users, so they are far less likely to fall prey to the various ploys from attackers.

Why HolistiCyber?

1. **Nation-state grade expertise** - our staff of white-hat security experts are former military and government offensive practitioners who can examine the attack surface from the **vantage point of the attacker** and not only from the vantage point of the company. This includes a solid grasp of the **sophisticated tooling** available to today's attackers and access to those attack tools.
2. **Holistic approach** - compliance, remediation, and mitigation solutions are tied to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.



"HolistiCyber is certainly our trusted advisor. Their professionalism, deep technical knowledge, and holistic approach have helped us meet our specific cyber security awareness objectives."

CISO, Hospitality and Resorts Corporation, USA