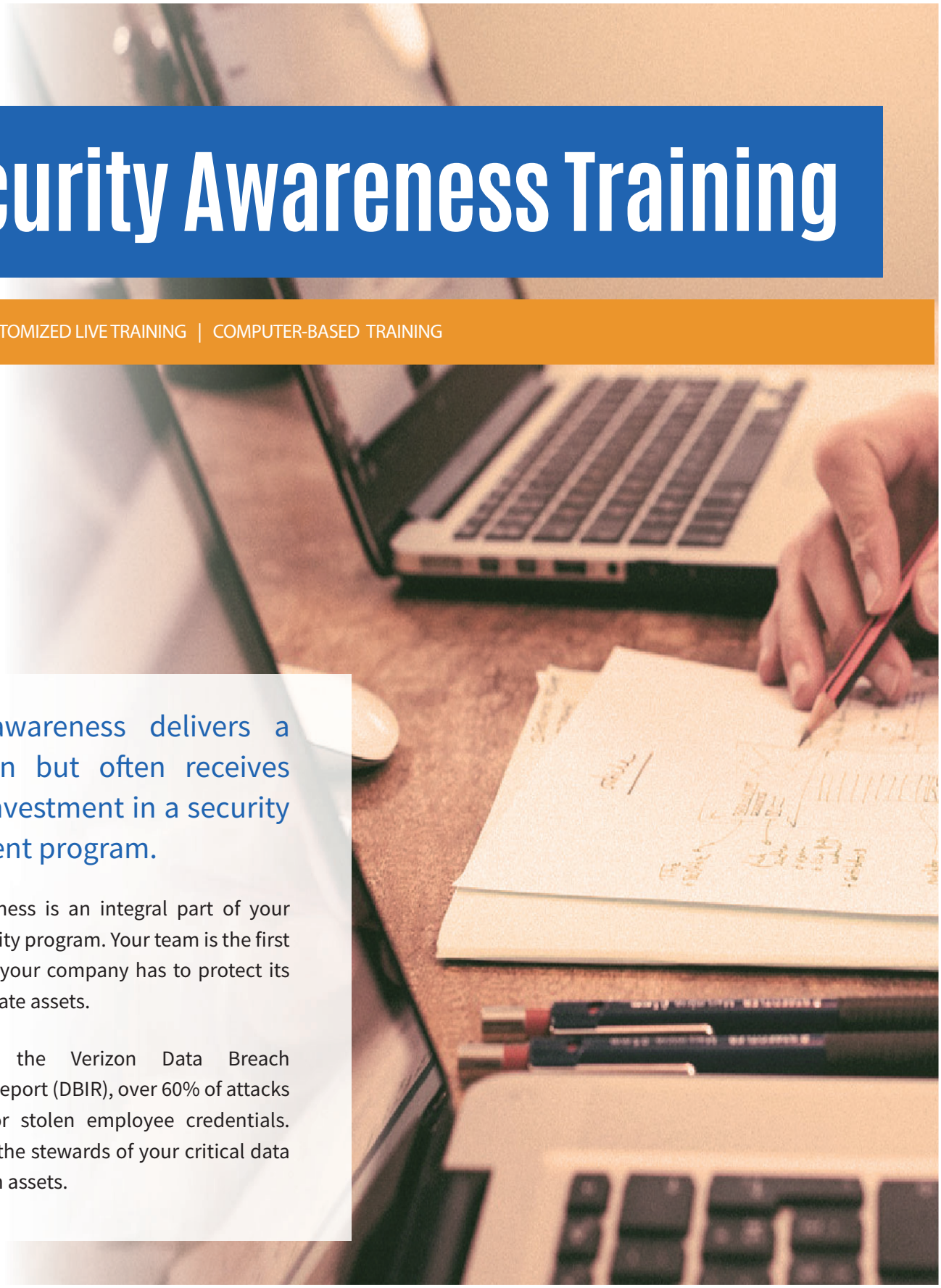
Security Awareness Training

CUSTOMIZED LIVE TRAINING | COMPUTER-BASED TRAINING



Security awareness delivers a high return but often receives the least investment in a security management program.

Security awareness is an integral part of your corporate security program. Your team is the first line of defense your company has to protect its valuable corporate assets.

According to the Verizon Data Breach Investigations Report (DBIR), over 60% of attacks exploit weak or stolen employee credentials. Employees are the stewards of your critical data and information assets.

HALOCK®

HALOCK Knows Training

Why do organizations need Security Awareness Training?

Compliance Many regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS 12.6), require a security awareness training program in order to achieve compliance. *Security Awareness Training is also included in best practice standards such as NIST and ISO.*

Executive Management Support Creates a holistic security message throughout an organization and facilitates awareness and acceptance from all employees regarding your security policies and procedures.

Common Security Language Defines security for all employees in terms that are relevant and appropriate for their roles, environment and corporate culture from operations, IT, human resources, and beyond.

Risk Management Making users aware of cyber threats and common vulnerabilities that are generally exposed by user actions minimizes exposure to threats and reduces liability.

Security Training Deliverables

Your Learning Experience Resources	Customized Security Awareness Training	Computer-Based/ eLearning Training
Live, instructor-based or video format training	●	
Access to online training modules		●
Digital files of training materials (guides, examples)	●	●
Quick Reference Job Aids which summarize training	●	●

Based on Your Learning Requirements

Every organization has their own training needs, which is why HALOCK offers a variety of options.

Customized Security Awareness Training

HALOCK meets with your team to define objectives, learning goals, and requirements to develop customized training for your organization. Based on HALOCK's tried and true best practices, the training material is customized to align to your established policies and procedures. This is especially important for organizations that may have to align to specific standards or regulations, or may have specific tools or processes that need to be highlighted. The material is also branded to your organization, examples included in the training are organization specific – bringing the lesson "home" for users. The framework of the training is "scenario-based" where attendees will be provided with Cyber Rules & Safe Practices for common scenarios attendees will find themselves in. Periodic Knowledge Checks engages participation with attendees.

FORMAT: Live, instructor-based or video format

Computer-Based Security Awareness Training

For organizations that simply need an overview of security awareness education for their teams, HALOCK offers an off-the-shelf computer-based course work option. Computer-based training is offered on a per-user basis. This is an efficient and effective option for businesses to meet compliance requirements.

FORMAT: Computer-based

Other Training Options

As part of our comprehensive Incident Readiness Solution, HALOCK offers training to help your team be prepared for any security incidents. We train your team on the established incident response safeguards and protocols.

INCIDENT RESPONSE TEAM TRAINING: Ensure that your Incident Response team members are familiar not only with your Incident Response Plan, but also with their roles and responsibilities during a security incident as well as with the communication processes both inside and outside the organization. Includes a review of the basics as well as tabletop exercises.

FIRST RESPONDER TRAINING: Includes high-level technical skills, survey of best practices and an overview of legal requirements that your first responders need in order to limit the data loss, overall impact and spread of an incident.

Common Custom Training Topics

People

Privacy
Social Media
Social Engineering
Insider Threat

Process

Laws and Regulations
Policies & Procedures
Physical Security
Incident Response
Password
Outside the Office/Travel

Technology

Malware
Email/Instant Messaging
Websites
Mobile Device
Phishing
Spear-phishing
Whaling
Business Email Compromise (BEC)
Cloud
Home Network
Ransomware

Common Custom Training Scenarios

Each of these is broken down to the Prevalent Attacks for each scenario, then Cyber Rules and Safe Practices will be discussed for each, as well as introducing various Concepts and showing attack Case Studies.

Scenarios

- Unknown/Fraud Phone Call
- Surfing the Web
- Using Social Media
- Emailing
- Out of the home/office (and using Wi-Fi)
- On Mobile Phone
- Ensuring compliance
- Working with money/Wire Transfers
- Accessing online accounts
- Using phone and web applications
- Setting up your home network

Common Attacks Discussed

- Social Engineering
- Drive-By-Download
- Malware/Adware/Spyware
- Ransomware/Scareware
- Phishing/Spear-Phishing/Smishing/Whaling
- Extortion/Theft
- Traffic Capture (Wi-Fi Eavesdropping)
- Rogue Wi-Fi (Evil Twin)
- ARP Poisoning (Man in the Middle)
- Insider Threat
- Cyber Security Incidents
- Business Email Compromise
- Password Attacks

Concepts Reviewed

- Data Classification Categories
- Attack Approaches
- Virtual Private Network (VPN)
- Cyber Security Incident Examples
- Multi-Factor Authentication
- Using Authenticators for MFA

Why HALOCK?

HALOCK combines the thought leadership and deep technical expertise with a proven ability to get things done. When you partner with HALOCK, you get not only the best and brightest in the field, but also the most capable. Simply stated, we get it right and we get it done.

As principal authors of **CIS Risk Assessment Method (RAM)** and board members of The **Duty of Care Risk Analysis (DoCRA)** Council, HALOCK offers the unique insight to help organizations define their acceptable level of risk and establish "duty of care" for cybersecurity. Through this risk assessment method, businesses can evaluate cyber risk that is clear to legal authorities, regulators, executives, lay people, and security practitioners.

HALOCK's service philosophy, **Purpose Driven Security®**, can best be summarized as reasonable and appropriate risk management:

Security controls implemented should encompass the necessary **balance of compliance and business goals.** Not all security controls should be implemented, and those that are should be implemented only to a certain degree depending on the calculated risk being treated.

Organizations have an obligation to **perform proactive due care to reduce liability for shareholders, clients, partners, employees and the greater good** as appropriate. Thus, businesses need to take into consideration on cyber threats that are foreseeable, which HALOCK can help identify.

This comprehensive approach enables organizations effectively support a security budget and maximize protection of critical information assets.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

www.halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.