CAMPUSGUARD®

Developing an Effective Security Awareness Training Program

Presented By:

Katie Johnson, PCIP
Product Lead – Online Training
Sr Customer Relationship Manager
CampusGuard

Margaret Gokturk
QSA, CISSP, CISA, GLEG
Security Advisor
CampusGuard

Chad Wheeler
OSCP, CEH, CISSP, PCIP, ASV
Manager, RedLens Infosec, a Division of CampusGuard

CAMPUSGUARD®

REDLENS INFOSEC™

A Division of CampusGuard

Agenda

- Identifying Risks
- Meeting Compliance Requirements
- Quality Training Content
- Frequency of Training and Ongoing Updates
- Gaining Support and Enforcement
- Measuring Effectiveness and ROI

Identifying Risks

Use your risk assessments to:

- Identify immediate risks facing your organization
- Prioritize areas or systems of significant risk
- Identify specific data types of higher risk
- Identify employees responsible for accessing systems/data

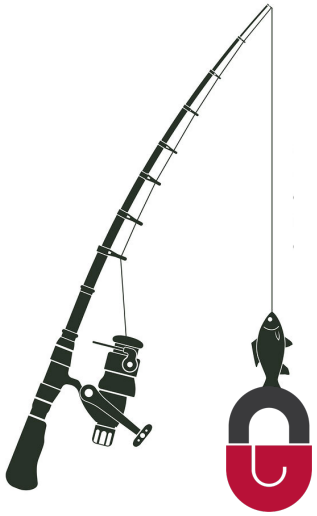
Risks: Phishing

61% increase in the rate of phishing attacks

- Emails from unknown senders
- Clicking on fraudulent links / opening attachments
- Significant increase in attacks on mobiles

TRAINING:

- How to recognize warning signs of an attack
- Everyone is responsible, not just IT
- No rushing through email at the end of the day, before a holiday, etc.



Risks: Social Engineering

- Impersonating a co-worker/boss
- Information gathering
- Emotions – urgency, greed, curiosity, helpfulness, and fear

TRAINING:

- Documented procedures on who has access to what
- Outlined approval processes
- Visitor management
- Incident reporting

Risks: Bad Password Habits

- Are we embarrassed that ‘password’ is still the most commonly used password?
- Using the same password across multiple websites

TRAINING:

- Creating secure passwords/ passphrases
- Required password changes
- Password management

PARTICIPANT POLL

Risks: Vulnerable Document Processes

Printing sensitive information

Leaving sensitive information on desks

Storing sensitive documents on servers, file shares, personal accounts

Emailing sensitive information

TRAINING:

- Protecting paper documents
- Storing in approved locations
- Encrypting communications or using approved methods to transmit sensitive information

Risks: Third-Parties

Breaches caused by compromised vendors	**20%**
Average cost of a breach	**$4.46 million**
Organizations with vendor inventory	**33%**

TRAINING:

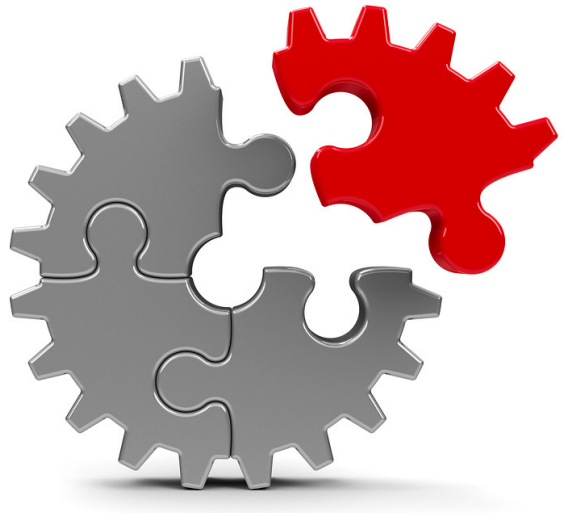
- Policy for contracting only with vetted/approved vendors
- Monitoring vendor security and compliance ongoing
- Incident response/management for third-party compromise

Compliance Requirements

PCI DSS	
v3.2.1	General infosec awareness at hire and annually.
v4.0	Training must include phishing and social engineering threat awareness, focus on CDE risks, acceptable use training for end user technologies (email, laptops, etc.); annual updates.
GLBA	
All Staff	Annually and updated as needed based on specific threats identified in risk assessment.
Job-Specific	Significant level appropriate for Qualified Individual; knowledge of infosec personnel reflects current threat landscape.
HIPAA	
All Staff	Periodic training – awareness and training program for all workforce members to ensure the security and privacy of PHI.
CMMC	
NIST 800 171 r2	Organizational system users are trained on infosec risks and consequences of actions and associated policies for use.
NIST 800-172	Employees are trained to recognize/respond to current threats such as advanced persistent and insider threats, behaviors and social engineering techniques – includes exercises and effectiveness.
FACTA Red Flags	
All Staff	Training to ensure all staff/employees can effectively address red flag issues; prevent and mitigate identity theft.

Training Content

- High quality content
- Applicable to employees' personal and professional lives
- Applicable to remote/hybrid work environments
- Risks and best practices
- Customizable/aligns with policy and procedure
- Targeted to specific roles/responsibilities
- Engaging and interactive
- Empowers decisions/behavior change



Frequency/Updates

- On-boarding
- Ongoing (quarterly, monthly)
- Smaller, micro-modules
- Targeted campaigns
- Supplemental resources
- Ongoing evaluation
- Staff feedback

Enforcement/Support

- Need executive buy-in? Leverage compliance!
  - GLBA board updates
  - Show the impact of an incident
    (never waste a good crisis)
  - Share risk assessment results to show likelihood
  - Request resources to support training requirements

Measuring effectiveness

Metrics:

- Reduction in system downtime or network/application outages
- Reduction in malware outbreaks and PC performance issues
- Reduction in resources spent responding to compromised machines (help desk tickets)
- Increase in reporting/questions
- Increase in number of personnel completing training
- Increase in comprehension (quizzes/training assessments)

*Also great information for your required, annual written report to the board!

Measuring effectiveness

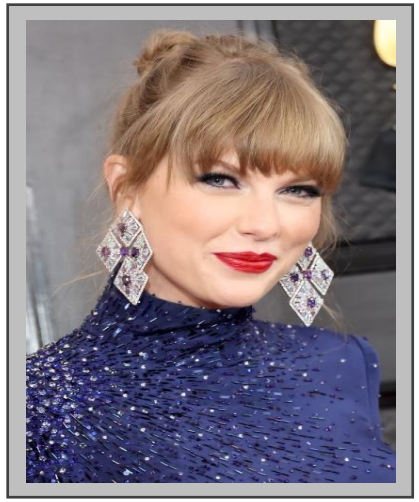
- Phishing staff
- Password auditing

Questions?

If ____ Ran Your Infosec Awareness Program

A. Beth Dutton

B. Tiger King



C. Taylor Swift

D. ??????

Contest details on the CampusGuard Blog:

Send entries to: marketing@campusguard.com