TRAINING FOR GOLD
How to Make PCI DSS Assessments Stress-Free

Tiana B. Clewis, President

Boyd Clewis, Vice President

Baxter Clewis Consulting

Scott Davis, Senior PCI Assessor

Frazier & Deeter

150B

SPENT ON CYBERSECURITY SERVICES IN 2021

Gartner Report May 2021

67%

SUCCESSFUL EXFILITRATION ATTACKS

Verizon Payment Security Report (2020)

53%

SUCCESSFUL UNDETECTED ATTACKS

Verizon Payment Security Report (2020)

91%

ATTACKS DID NOT GENERATE ALERTS

Verizon Payment Security Report (2020)

TIANA B. CLEWIS

President
BAXTER CLEWIS CONSULTING
tiana@baxterclewis.com

PCI Security Standards Council®

BOYD CLEWIS

CISSP, CISA, CCSK, PCIP

Vice President

BAXTER CLEWIS CONSULTING

boyd@baxterclewis.com

PCI Security Standards Council®

SCOTT DAVIS

CISSP, CISA, PCIP

Senior PCI Assessor

FRAZIER & DEETER

scott@integritynetworks.org

PCI Security Standards Council®

Training for Gold

AGENDA

- Learning Objectives
- Reality vs. The Gold Standard
- Recommendations

PCI Security Standards Council®

Training for Gold

LEARNING OBJECTIVES

- Uncover how current training models are leaving your company vulnerable to breach and compliance failures
- Discover ways to reduce the failure rate of time-based PCI DSS requirements
- Learn key strategies to improve the timeline and efficiency of your annual PCI DSS assessment without investing in new tools and software

PCI Security Standards Council®

Training for Gold

THE REALITY OF MANY ORGANIZATIONS

- People – Lacking adequate training
- Processes – Not aligned with security best practices
- Technology – Heavy investment with limited return

PCI Security Standards Council®

Training for Gold

THE REALITY OF MANY ORGANIZATIONS

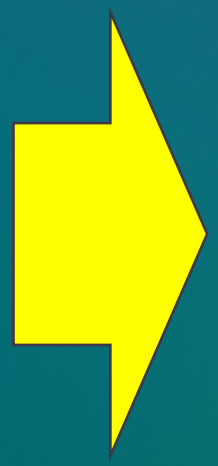
- Increased assessment duration
- Intense anxiety at all levels of the organization
- Failure of time-based PCI DSS requirements
- Increased assessment cost due to remediation
- Increased risk of a costly security incident

PCI Security Standards Council®

There Is a Better Way!

PCI Security Standards Council®

PCI DSS ASSESSMENT DURATION (2020 vs. 2021)

12months  8months

Training for Gold

THE GOLD STANDARD

- A culture of **Compliance** can lead to a state of **Security**:
  - Team members understand the impact and relationship of their role with PCI DSS compliance
  - Maintaining compliance is a natural part of how your company does daily business
  - Detecting and addressing compliance issues is treated as a business imperative instead of an inconvenient side-project

PCI Security Standards Council®

Training for Gold

RECOMMENDATIONS: CONDUCT ROLE-SPECIFIC TRAINING

- Common risk and vulnerabilities
- Applicable PCI DSS requirements
- Company processes and procedures for PCI DSS requirements
- Security best practices

PCI Security Standards Council®

Training for Gold

RECOMMENDATIONS: DOCUMENT COMPLIANCE-BASED SOPS

- Clear, accurate, and accessible
- Communication of SOP changes
- Periodic review schedule
- Last revision date

PCI Security Standards Council®

Training for Gold

RECOMMENDATIONS: ESTABLISH ACCOUNTABILITY SYSTEMS

- Assign responsible parties for each process
- Periodic review of specific processes and evidence
- Collect and maintain evidence

PCI Security Standards Council®

Training for Gold

RECOMMENDATIONS: APPOINT A PCI DSS CHAMPION

- PCI DSS subject matter expert (SME)
- SME advisory on all CDE impacting changes
- Authority to address compliance issues
- Develops training and enhancements to the compliance program

PCI Security Standards Council®

TRAINING FOR GOLD
How to Make PCI DSS Assessments Stress-Free

Tiana B. Clewis, President

Boyd Clewis, Vice President

Baxter Clewis Consulting

Scott Davis, Senior PCI Assessor

Frazier & Deeter