NC Public Health HIPAA Alliance

23-June-2017

HIPAA Security Risk Assessment - Why

Carolinas IT
Experience
Peace of Mind

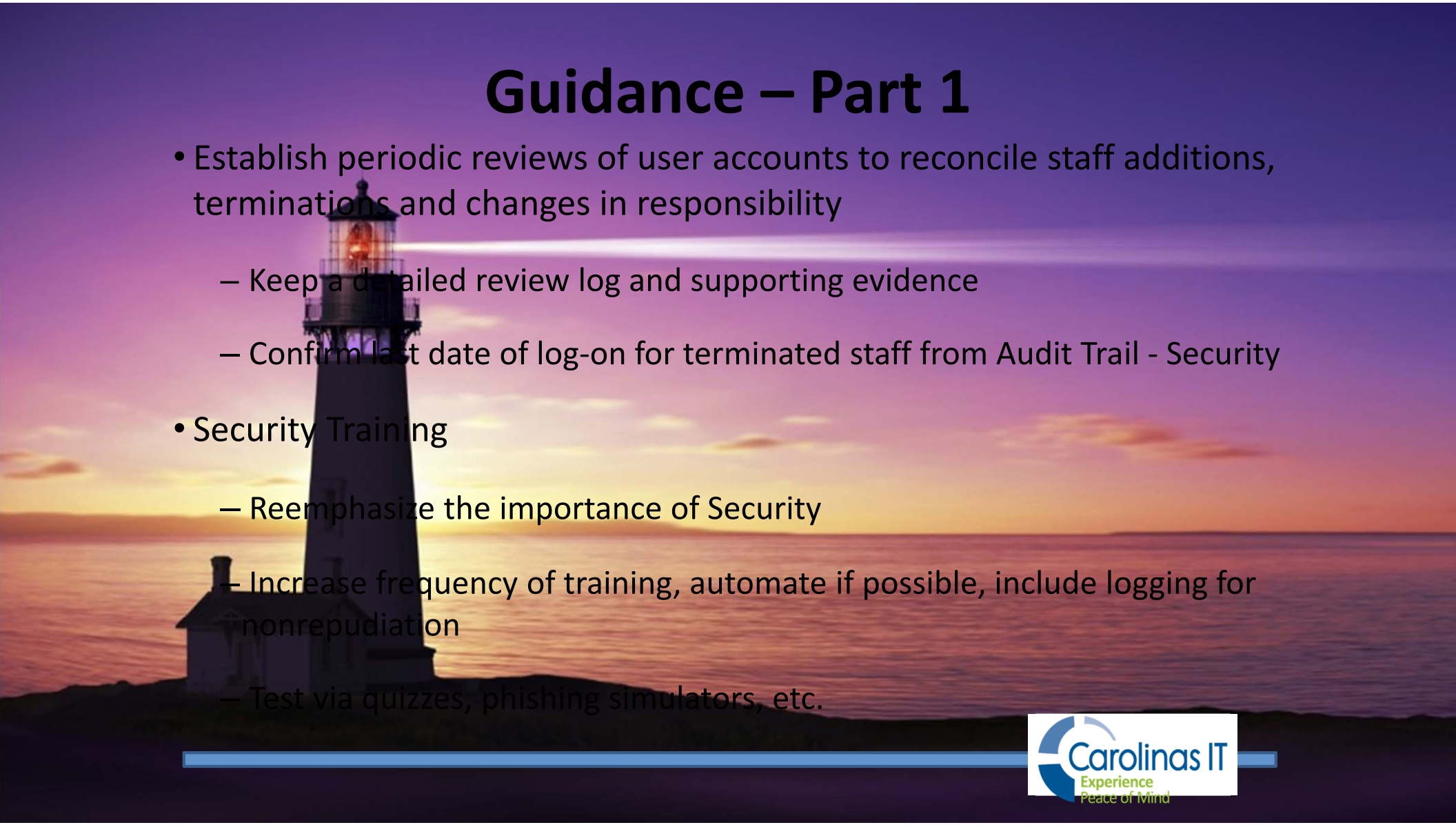
Top Risks to Security of ePHI

- End-users' lack of security training
- Failure to manage user accounts
- Failure to use designed security controls e.g. session time-out, password complexity, password expiration, role-based access
- Failure to harden the instance after deployment/failure to patch
- Negligent management of business associates
- No backup, no redundancy
- No encryption

Carolinas IT
Experience
Peace of Mind

Guidance – Part 1

- Establish periodic reviews of user accounts to reconcile staff additions, terminations and changes in responsibility
  - Keep a detailed review log and supporting evidence
  - Confirm last date of log-on for terminated staff from Audit Trail - Security
- Security Training
  - Reemphasize the importance of Security
  - Increase frequency of training, automate if possible, include logging for nonrepudiation
  - Test via quizzes, phishing simulators, etc.



Guidance – Part 2

- Test Technical Vulnerabilities
  - External Penetration Test
  - Internal Penetration Test
  - On-site Social Engineering
- Revise Security Incident Response and Breach Notification Procedures

Carolinas IT
Experience
Peace of Mind

Carolinas IT SRA Approach

The Goal: to reveal the areas where your ePHI is at risk and recommend steps to reduce that risk

- Diagnostic Tools (vulnerability, AD scans)
- Checklists
- Professional Reports
- Guided by an ISACA Certified Information Systems Auditor following industry standards
- Penetration Testing, Phishing, OSE (optional)

Carolinas IT
Experience
Peace of Mind

The Carolinas IT Difference

- 14 NC Public Health customers (CureMD, Patagonia, NetSmart)
- Comprehensive Review of Controls, Policies and Procedures is included in the Standard SRA
- CIT SRAs are lead by auditors who were IT Directors
- CIT provides Policy and Form templates
- CIT conducts Progressive Assessments
  - Increasing level of focus on controls
  - Periodic audit of critical controls: Training Records, User Account Management and Evidence of Activity Log Review

Carolinas IT
Experience
Peace of Mind

- _____ are a company's biggest security risk.
- _____ _____ should be completed periodically in order to keep users up-to-date and aware of the evolving threat environment.
- _____ _____ allows you to gain an understanding of which vulnerabilities are most likely to be exploited by a threat.
- The Carolinas IT SRA approach provides a picture of risk and a _____ _____ to help you design a security roadmap.

Thank You!

R. Greg Manson

Director of Audit and Compliance

Greg.Manson@CarolinasIT.com, 919-573-4084

1600 Hillsborough Street
Raleigh, NC 27605

www.CarolinasIT.com

Carolinas IT
Experience
Peace of Mind