

Carolinus IT
Information Technology
Hospital of Wake

HIPAA Security in a World of Cybersecurity Risk

Presented by: R. Greg Manson
Director of Security, Audit and Compliance, Carolinus IT

Carolinus IT
Information Technology
Hospital of Wake

Cyber Risk = Potential for Loss

Carolinus IT
Information Technology
Hospital of Wake

Cyber Risk = Threat + Vulnerability

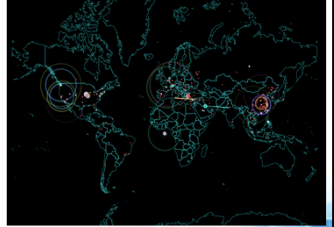
*Infosec Institute

Carolinus IT
Information Technology
Hospital of Wake

Threats

"Anything that can exploit a vulnerability, intentionally or accidentally"

- Threat Actors
- Malware
- Insiders/Users
- Phishing



Carolinus IT
Information Technology
Hospital of Wake

Vulnerabilities

"Weaknesses or gaps in security"

- Inadequate/Non-Existent Security Training
- Poor User Account Management
- Unpatched Software and Operating Systems
- Legacy, Atrophied Functionality

Carolinus IT
Information Technology
Hospital of Wake

Cyber Risk = Threat + Vulnerability

*Infosec Institute

Threat Stats

"Anything that can exploit a vulnerability, intentionally or accidentally"

- Threat Actors: \$1.5T in 2017 - RSA
- Malware: 350,000 New Programs Daily - AVTest
- Insiders/Users: 43% to 70% - Protenus
- Phishing: 156M Phishing Emails Daily - Canada DPS

Category	Percentage
Insider	43%+
Unknown	11%
Loss or Theft	19%
Outside Hackers	27%

Protenus/DataBreaches.net - 2016 Breach Barometer Report



Cyber Risk =

Threat + *Vulnerability*

*Infosec Institute

Vulnerabilities - NCPH

"Weaknesses or gaps in security"

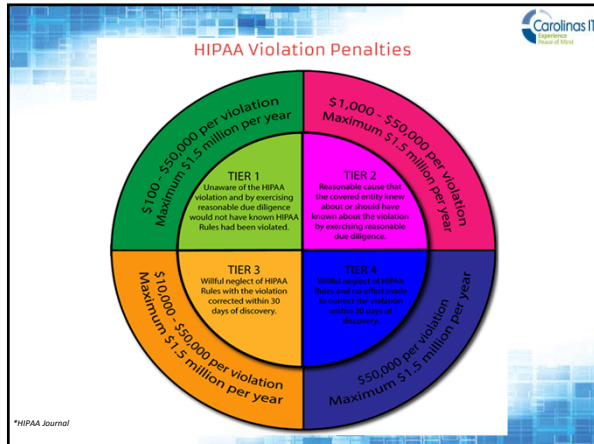
- Inadequate/Non-Existent Security Training
- Poor User Account Management
- Over-Privileged Users
- Weak Password and Log-Out Enforcement
- Insufficient Inventory of ePHI
- Mobile Devices and Surplus Hardware

The Real Risk...

HIPAA and the Security Rule

Timeline of HIPAA Regulations:

- 1996: HIPAA (Health Insurance Portability and Accountability Act)
- 2003: HIPAA COMPLIANCE (Privacy)
- 2005: HIPAA Security Rule (ePHI)
- 2009: HIPAA HITECH Compliance (Breach)
- 2013: HIPAA OMNIBUS (BA)



The Lesson
Control the User!

- TRAINING
- Employee Separation & Offboarding Checklist
- AGREEMENTS

Why Periodic Assessments?

- Required – Administrative Standard 164.308(a)(1)(i)
- Measures control effectiveness
- Documents progress on the Management Plan
- Identifies new risks
- Prepares for additional hardening
 - Internal/External Pen Tests
 - Wireless Test
 - Onsite Social Engineering
- Prepares for expansion to other departments

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