Implementing Multi-factor Authentication for Clinical Applications

Presented by:
Todd Greene (Carolinas Healthcare System)
Jon Sternstein (Stern Security)

Carolinas HealthCare System

Introduction

- Jon Sternstein, Founder & Principal Consultant – Stern Security
- WakeMed – Former Data Security Manager
- Co-Chair of NCHICA Technology Workgroup
- SANS Institute – Mentor
  - Teach SANS 560 Network Penetration Testing and Ethical Hacking
- Industries: Healthcare, Finance, Government, Education
- Certifications – CISSP, GPEN, Certified Ethical Hacker, CCNA, and more…
- I love Multi-factor authentication ☺

INTRODUCTION

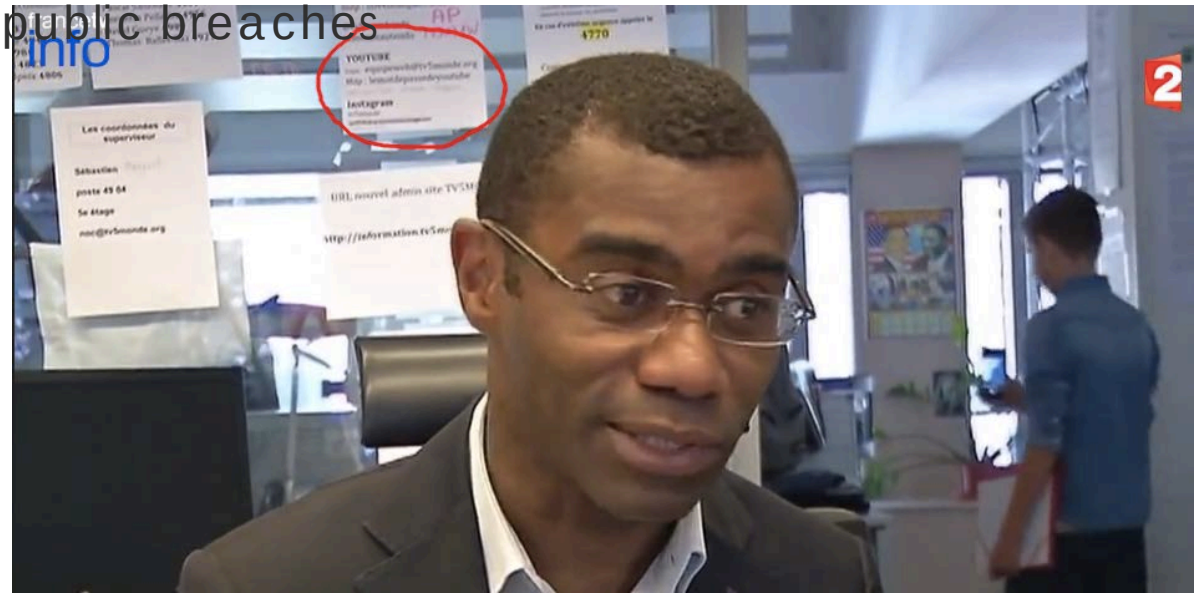
- Todd Greene – Manager, IS Governance, Risk and Compliance
- 17+ years of service
  - Started as a Windows NT & Novell 3.12 Admin
  - Moved to IS Security a year later and have been there since
- Co-Chair of NCHICA Privacy and Security Workgroup
- Certifications – CISSP & PCI ISA
- A big proponent of the use of multi (2) factor authentication

What is Multi-factor Authentication?

- One of the most powerful security features
- Demonstration
  - Could you access my account if you stole my password?
- Two out of the three options:
  - Something you KNOW (e.g. password, PIN)
  - Something you HAVE (e.g. phone, badge, card, RSA token)
  - Something you ARE (e.g. fingerprint, retina scan, heartbeat)

Why Multifactor?

- Required to e-prescribe controlled substances
  - DEA requirement: http://www.deadiversion.usdoj.gov/fed_regs/rules/2010/fr0331.htm
- Easy to steal passwords
  - Phishing, passwords written down, guessable passwords, network attacks, public breaches
- Best Practice

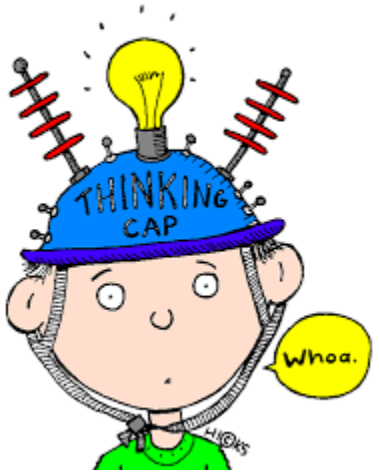


Where to Implement Multifactor?

- Remote Access VPN
- EHR
- External (Cloud based) Clinical Applications
  - Limit access to organization's network

THINGS TO THINK ABOUT

- What services do you have today that are exposed to the Internet?
  - Are you sure you know where everything is and what is out there?
- I'd suggest using your last external penetration test (or have one conducted)
  - This will ensure you don't miss something
  - Review the list carefully…..What is there that I may be missing?
- Maybe a few examples would help….

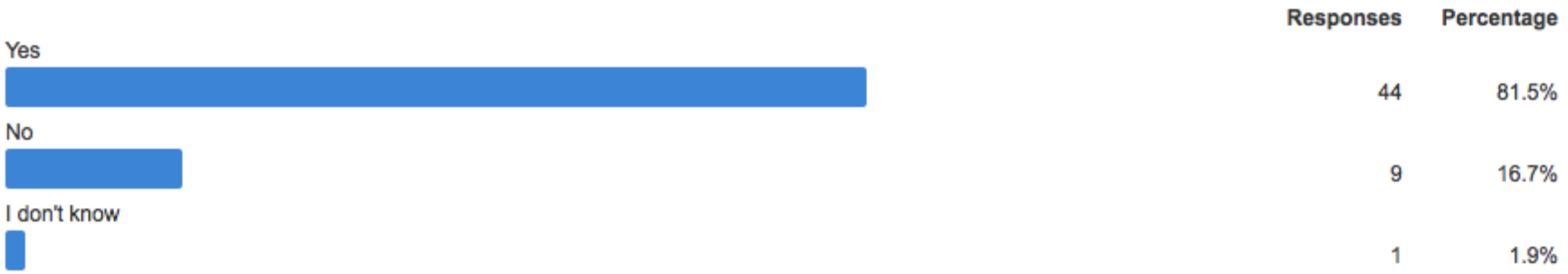


DO ANY OF THESE LOOK FAMILIAR?

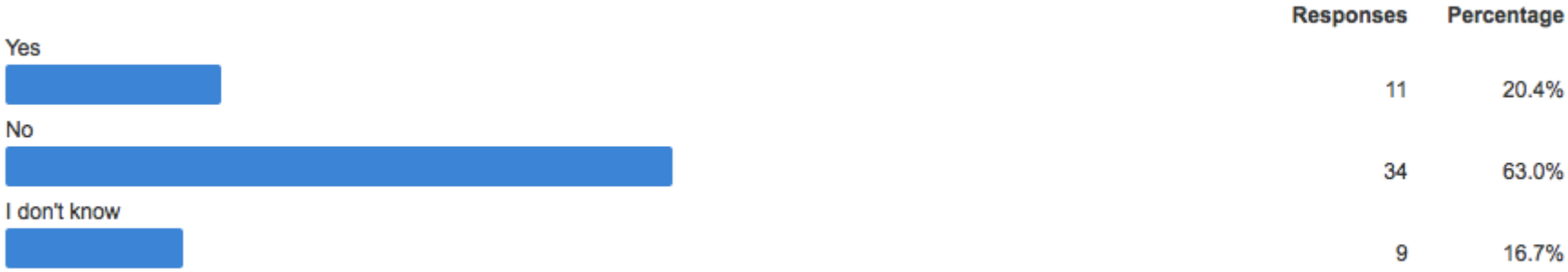
- Human Resource Portals
- Electronic Timecard Portals
- Remote access systems
- Web-based mail systems
- Secure web-based mail systems
- Scheduling systems
- Internal websites (intranets, etc.)

Statistics from NCHICA Technology Workgroup

- Do you allow your providers to remotely access your EHR?



- Does your organization utilize 2-factor Authentication?



How to implement 2-factor?

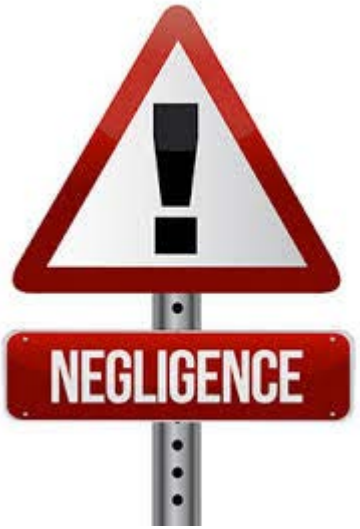
- 1. Secure Personal Accounts First
  - Create workshops
  - Gmail, Outlook/Hotmail, Yahoo!, Twitter, Facebook, LinkedIn, Apple
- 2. Configure on test systems
- 3. Configure on production systems
  - A. Start with optional enrollment for specific groups
  - B. Expand group membership
    - Give away prizes
  - C. Enforce enrollment

Multi-factor Authentication Solutions

- Duo
- RSA
- Microsoft
- Custom code - TOTP (Time-based One-time Password Algorithm)
- And many, many others

WHY THE URGENCY

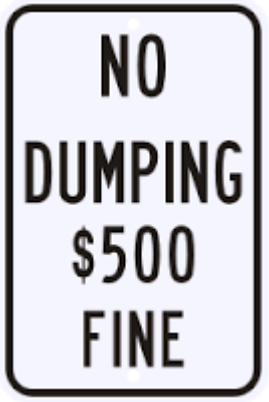
- As mentioned before, phishing is a major problem and an ever growing threat.
  - Once phished, the attacker has direct access to your data without two-factor authentication
    - EMR, Email w/ Attachments, PII (NCITPA), etc.
    - If used, transmission encryption doesn't matter
    - Is the user accessing the system "authorized"?
    - Can you guarantee the data was modified?
- Due to the potential OCR fines of a violation.
- Since two-factor is now an industry best practice, could a violation be considered willfully negligent?
- Let's go down that road and see where it leads.



POSSIBLE HIPAA RULE VIOLATIONS

- 164.308(a)(4)(i) Information access management
- 164.308(a)(4)(ii)(B) Access authorization
- 164.312(a)(1) Access Control
- 164.312(a)(2)(iv) Encryption and Decryption
- 164.312(c)(2) Mechanism to authenticate EPHI
- 164.312(d) Person or entity authentication
- 164.312(e)(1) Transmission security
- 164.312(e)(2)(i) Integrity controls
- 164.312(e)(2)(ii) Encryption

WHAT'S THE FINE?



- Fines are capped at 1.5M per rule violation for willful negligence
  - Best case: 2 rules violated = $3M fine
  - Worst case: 9 rules violated = $27M fine
- Have you noticed the fines being accessed lately. They are in the $1M-5M range.
  - And don't forget the fines are what fund the program!
- Don't forget about civil fines
  - Yes, they can even come after you as an individual
  - Follow your institution's policies and you'll likely be fine there.

Additional Measures

- Limit further changes to password policy
  - Password length
  - Password expiration
- https://twofactorauth.org
  - List of services that support 2-factor authentication.
  - Contact companies that have not implemented 2-factor authentication
- Strength in numbers
  - Healthcare organizations can request 2-factor support from their vendors.

Carolinas HealthCare System

Questions?