# HIPAA SECURITY RISK ASSESSMENT

## AT 30,000 FEET

**JOHN HARMON**

**COO - FRSECURE**

FRSECURE™
INFORMATION SECURITY EXPERTS
www.frsecure.com

# AGENDA

Introduction / FRSecure Overview

Information Security Defined

Risk Assessments

Technical Assessments

People Assessments

Suggested areas to focus on

# WHO IS FRSECURE?

- Information Security Management Company
- Founded 2008
- Based in Minneapolis/St. Paul MN
- 50 People
- Product Agnostic
- Work Nationally
- Mostly Small/Middle-sized Companies
- All Industries
- VERY Proud of our Growth, Mission & Culture

MINNEAPOLIS/ST. PAUL BUSINESS JOURNAL
FAST50

2017 100 BEST COMPANIES TO WORK FOR 2017

# HIPAA SECURITY RULE

45 CFR 164.308 – Administrative Safeguards

- ii(A) Risk Analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of all electronic protected health information…

164.310 – Physical Safeguards

164.312 – Technical Safeguards

# STANDARDS REFERENCED BY HHS AND CMS

International Standards Organization (ISO) 27001/2 : 2013

National Institute of Standards in Technology (NIST) CSF / 800-53

- Administrative Controls
- Physical Controls
- Technical Controls (Internal & External)

# OCR AUDIT PROTOCOL

The Office of Civil Rights have published an audit protocol to investigate covered entities under HIPAA for compliance with both the Privacy and Security rules.

It's basically the ISO and NIST frameworks with a method of investigating the degree to which controls are implemented.

A corrective action plan or *CAP* is issued if deficiencies are found. Fines are common (in FRSecure's experience)

# SECURITY RISK 101

Risk = Likelihood + Impact + Maturity

Example: Laptops

Likelihood = High

Impact = High (depends on what info is on the laptop)

Maturity = High (if encrypted or something that effectively compensates)

Overall risk = Low due to maturity of compensating control.

# ADMINISTRATIVE CONTROLS

- Information Security Governance & Risk Management
  - How do we handle risk management and what is our risk tolerance
- Policies
  - What should we be doing
- Procedures
  - How should we be doing it
- Guidelines
  - Frameworks within which to implement procedures
- Standards
  - A mandatory action or rule designed to support and conform to a policy.
- Training
  - How do we let employees know what they should be doing and how to do it

| Control | Risk Management |
|---|---|
| 1.1 | Risk management practices and integration |
| **Control** | **Information Security Governance** |
| 2.1 | Policies for information security |
| 2.2 | Review of the policies for information security |
| 2.3 | Security roles and responsibilities |
| 2.4 | Segregation of duties |
| **Control** | **Human Resources Security** |
| 3.1 | Screening |
| 3.2 | Management responsibilities |
| 3.3 | Information security awareness, education, and training |
| 3.4 | Specialized information security education and training |
| 3.5 | Termination or change of employment responsibilities |
| **Control** | **Asset Management** |
| 4.1 | Inventory of assets |
| 4.2 | Classification of information |
| 4.3 | Management of removable media |
| 4.4 | Disposal of media |
| **Control** | **Access Control** |
| 5.1 | Access control policy |
| 5.2 | User registration and de-registration |
| 5.3 | Use of secret authentication information |
| 5.4 | Secure log-on procedures |
| **Control** | **Cryptography** |
| 6.1 | Policy on the use of cryptographic controls |

| Control | Security Operations |
|---|---|
| 7.1 | Mobile device policy |
| 7.2 | Teleworking |
| 7.3 | Documented operating procedures |
| 7.4 | Change management |
| 7.5 | Controls against malware |
| 7.6 | Information backup |
| 7.7 | Event logging |
| 7.8 | Installation of software on operational systems |
| 7.9 | Management of technical vulnerabilities |
| 7.10 | Information systems audit controls |
| 7.11 | Segregation in networks |
| 7.12 | Information transfer policies and procedures |
| 7.13 | Information security requirements analysis and specification |
| 7.14 | System acceptance testing |
| 7.15 | Information security policy for supplier relationships |
| **Control** | **Incident Management** |
| 8.1 | Incident management roles and responsibilities |
| 8.2 | Incident response procedures |
| **Control** | **Business Continuity Management** |
| 9.1 | Planning information security continuity |
| 9.2 | Recovery plan details |
| **Control** | **Compliance** |
| 10.1 | Identification of applicable legislation and contractual requirements |
| 10.2 | Privacy and protection of personally identifiable information |
| 10.3 | Independent review of information security |
| 10.4 | Compliance with security policies and standards |

# PHYSICAL CONTROLS

- **Crime Index**
- **Natural Disasters**
- **Secure Areas** (Datacenters, file rooms, etc.)
  - **Who's allowed in the IT closet? People steal servers (seriously).**
- **Equipment**
  - **Did you throw away that printer with the hard drive in it?**

# INTERNAL TECHNICAL CONTROLS

Behind the Firewall

- Network Connectivity
- Remote Access
- Directory Services
- Servers & Storage
- Client Systems
- Mobile Devices
- Logging, Alerting, and Monitoring
- Vulnerability Management
- Backup and Recovery

# EXTERNAL TECHNICAL CONTROLS

Internet-Facing Security

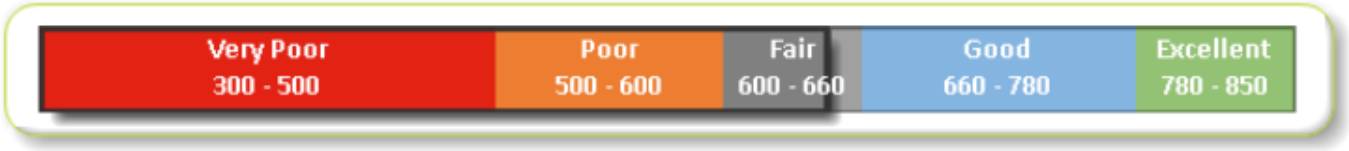
- Best Practices
- Reconnaissance
- Enumeration
- Vulnerabilities

# TECHNICAL ASSESSMENTS

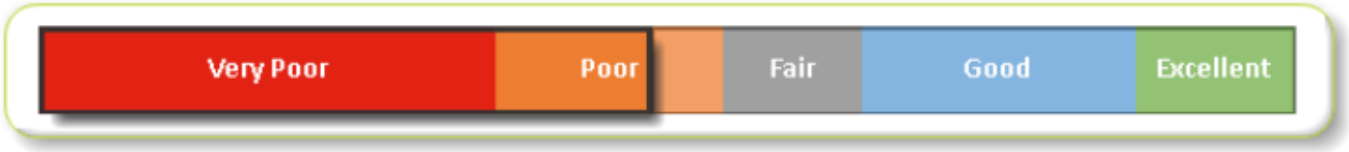
- Vulnerability Scanning
  - Internal & External Network
- Web Application Vulnerability Scanning
- Penetration Testing
  - Internal & External Network
- Web Application Penetration Testing

# OUTPUT SHOULD BE MEASURABLE

## FISASCORE™ Scale



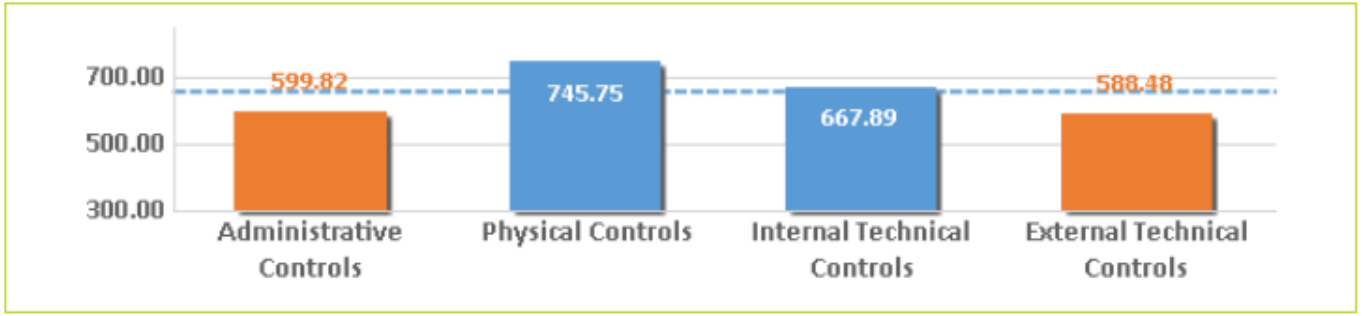

## FISA™ Industry Comparison




The average FISASCORE™ is 567.72. According to our calculations, there is roughly 13.7% less risk in the Client A information security program than other programs in similar organizations.

## FISA™ Phase-by-Phase Comparison

There are four phases in a Full FISA™ Assessment: Administrative Controls, Physical Controls, Internal Technical Controls, and External Technical Controls. An "acceptable" level of security is 660.



# VULNERABILITY SCAN VS PENETRATION TEST

# SOCIAL ENGINEERING IS HACKING PEOPLE


AND SOCIAL ENGINEERING IS

THE PATH OF LEAST RESISTANCE.

# ELECTRONIC – PHISHING/SPEAR PHISHING


- Phishing: click rate 14.13%
- Spear phishing: credentials obtained 23.23%
- Verizon Stat – 100/10/3

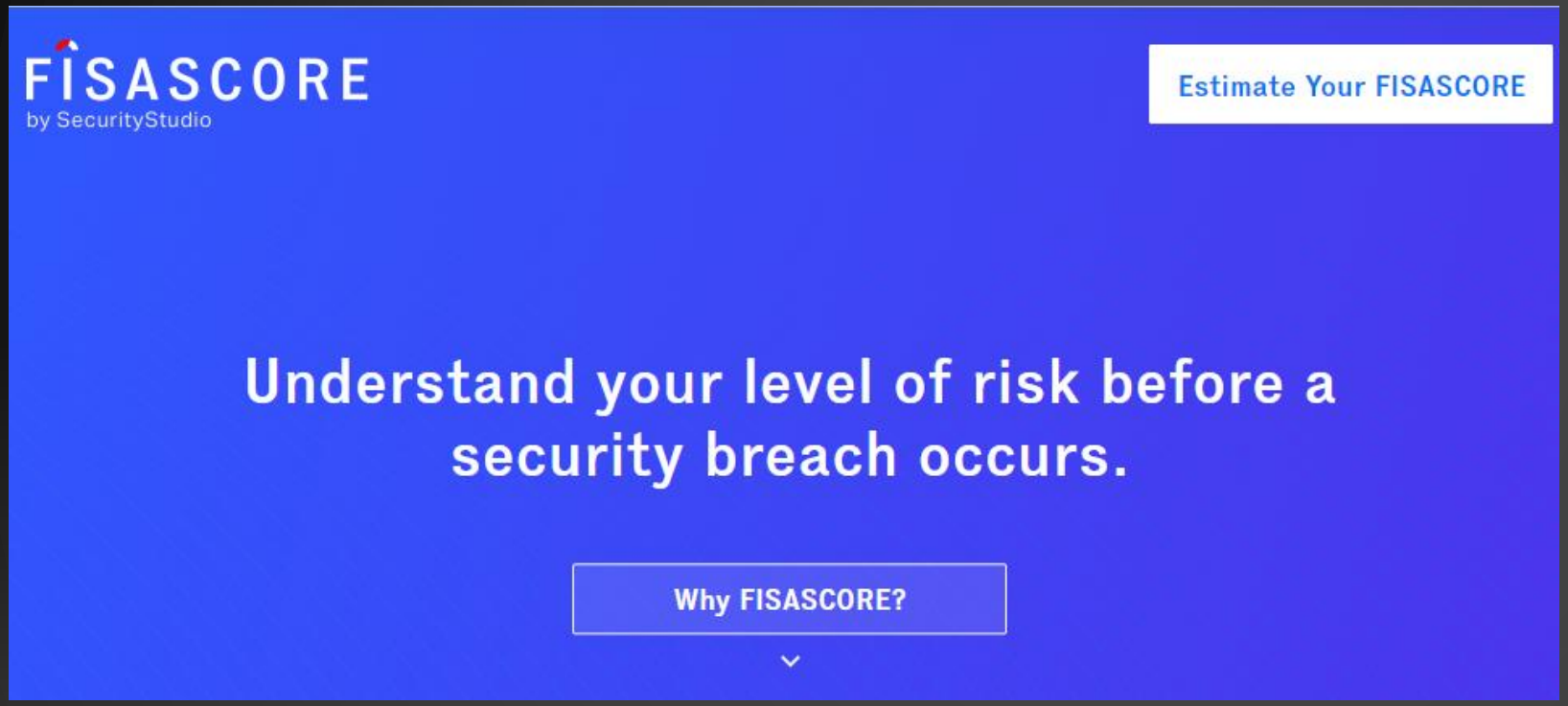
# PHYSICAL

- USB drop: software run on company system 8.33%
- Physical access: gained access to restricted or secure areas 100%

# FOCUS AREAS

- Asset Management
  - You can't protect what you don't know about.
- Vulnerability Management
  - 92% of known Microsoft vulnerabilities are 100% avoidable.
- Access Management
  - Do you know who has access to what and why?
- Incident Management
  - The worst time to find a problem is during an incident.
- Training
  - People are your biggest risk – get them up to speed!

# TAKE A FREE SELF ASSESSMENT




680+ is good

Get help!

FRSECURE.COM

# THANK YOU FOR YOUR TIME!

- For a free copy of this presentation and asset management tracker template please text “DRAKE18” to 44222.