# Healthcare Information Security Strategies:  Where to focus your limited efforts

April 2016

Saint Luke's
HEALTH SYSTEM

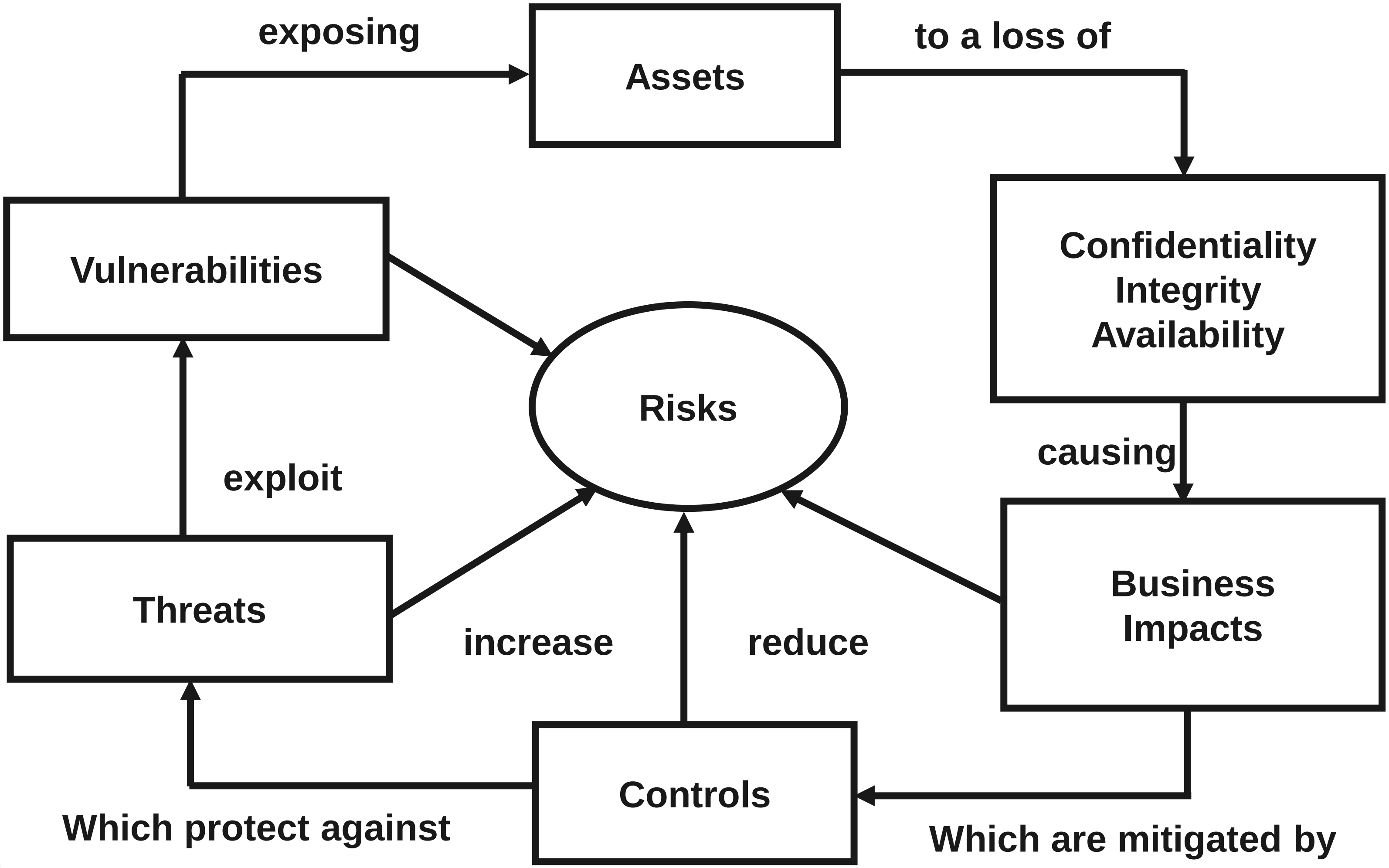
# Dave Wiseman
# Chief information Security Officer

- Over 25 years experience in the Security field
- SLHS Information Security since 2007
- Served as a Department of Defense Counterintelligence Agent / Cyber-Security Investigator
- Principal Security Engineer with the US Department of State assessing US Embassies throughout the world
- Manager of Information Security Operations at the US Agency for International Development
- Bachelors of Science from Regents College
- Certified Information System Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Department of Defense Trained Cyber Security Investigator

# Saint Luke's Health System

- Fully integrated  health system in metropolitan Kansas City
- 10 hospitals, 1,365 physicians, 65 specialty services
- Locally owned, not-for-profit, faith-based for 130 years
- Reputation for innovation, quality and compassion
- World class cardiovascular disease outcomes research
- One of nation's leading stroke reversal programs
- 10,000+ employees
- Serving patients in 65 counties in Missouri and Kansas

# Information Security Risk Cycle



Source: Unknown

THREATS

# Healthcare is now known as a very “SOFT” Target

| | |
|---|---|
| Anthem | 80 Million |
| Premera Blue Cross | 11 Million |
| TRICARE | 4.9 Million |
| Community Health | 4.5 Million |
| Advocate Health | 4.03 Million |
| Health Net INC | 1.9 Million |
| Blue Cross TN | 1.02 Million |
| AvMed Inc | 1.22 Million |

Recent Ransomware Events in the News:

- Hollywood Presbyterian Medical Center
- Kentucky Methodist Hospital
- Prime Healthcare Services
- Chino Valley Medical Center
- MedStar Health

VULNERABILITIES

# Healthcare Limitations

- Limited Budget
- Bio-Medical Devices
- Restrictions on Security Patching
- Physician / Clinician Need for Convenient "Patient Care"
- "Siloed" Environments
- Non-integrated Security Solutions
- Senior Management Buy-In
- "The Cloud"

CONTROLS

# Regulatory Requirements and Frameworks

Baseline Security

**Regulatory Requirements**

- HIPAA Security
- Joint Commission
- HITECH and Breach Rule
- FTC's Identity Theft Red Flag Rule
- State data breach notification acts
- PCI Data Security Standards

How To Guides

**Frameworks and Guidelines**

- FISMA-NIST (SP800-53)
- Sarbanes-Oxley
- NIST Cyber Security Framework
- CIS Critical Security Controls
- HITRUST Security Framework

CONTROLS

# NIST Cyber Security Framework

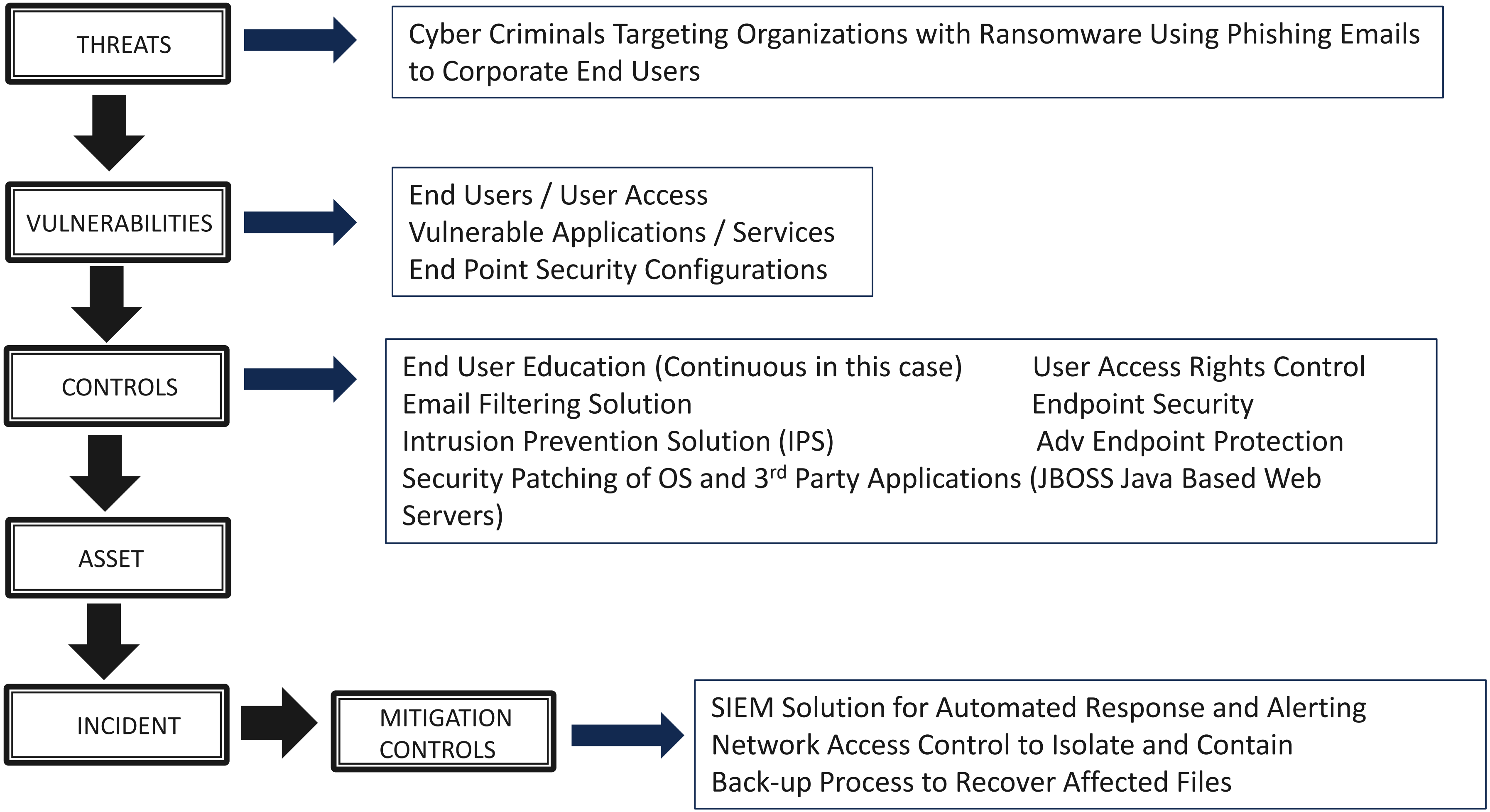
| FUNCTION | CATEGORY |
|---|---|
| IDENTIFY | Asset Management |
| | Business Environment |
| | Governance |
| | Risk Assessment |
| | Risk Management Strategy |
| PROTECT | Access Control |
| | Awareness and Training |
| | Data Security |
| | Information Protection Processes and Procedures |
| | Maintenance |
| | Protective Technology |
| DETECT | Anomalies and Events |
| | Security Continuous Monitoring |
| | Detection Processes |
| RESPOND | Response Planning |
| | Communications |
| | Analysis |
| | Mitigation |
| | Improvements |
| RECOVER | Recovery Planning |
| | Improvements |
| | Communications |

- Admin Controls
- Governance /Awareness
- Risk Cycle Process

- Technical Controls (Detection/Prevention)

- Incident has occurred
- Mitigation controls
- Recovery Process
- Lessons Leaned – Additional Controls

# Walking it through…



THREATS

Cyber Criminals Targeting Organizations with Ransomware Using Phishing Emails to Corporate End Users

VULNERABILITIES

End Users / User Access
Vulnerable Applications / Services
End Point Security Configurations

CONTROLS

End User Education (Continuous in this case)
Email Filtering Solution
Intrusion Prevention Solution (IPS)
Security Patching of OS and 3rd Party Applications (JBOSS Java Based Web Servers)

User Access Rights Control
Endpoint Security
Adv Endpoint Protection

ASSET

INCIDENT

MITIGATION CONTROLS

SIEM Solution for Automated Response and Alerting
Network Access Control to Isolate and Contain
Back-up Process to Recover Affected Files

# Limited Resources – What to do?

- Build the base of a security program and continue to mature it
- Get Leadership on board
- Deal with low hanging fruit – outside in approach
- Centralized vs. Distributed Security responsibility
- Out running the bear
- Situational Awareness is key function
- User Awareness – KEY “Culture Change”

# Keep Your End Users engaged in Security

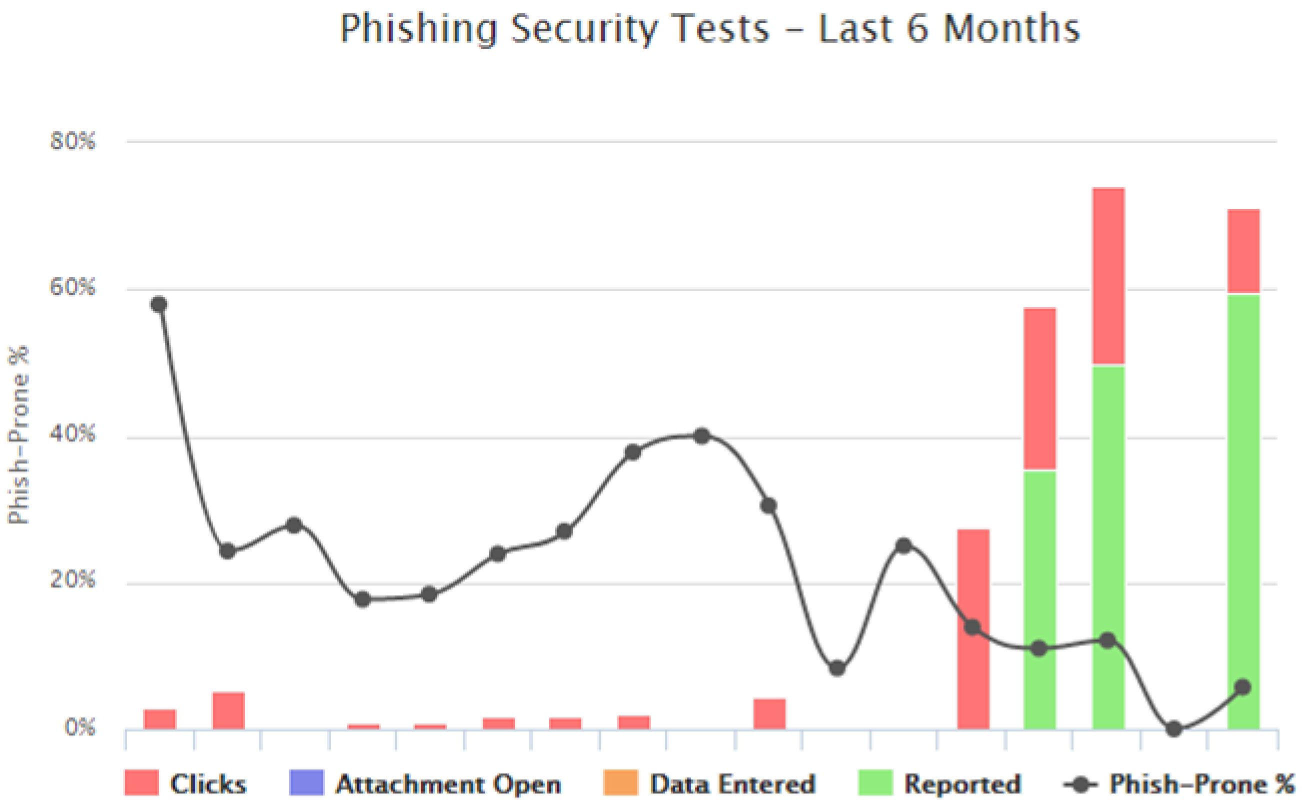
- **New Hire Orientation for all new employees**
  - Focus on real-world cyber events and the employees being the “target”
  - Follow-on written security test complete first 30 days
- **Annual Compliance Training (ACT) Security Module**
  - Reviewed and updated annually based on real-world cyber events
  - Can be ineffective since it is annual – reserve for regulatory / policy training
- **Security Awareness Articles / Emails**
  - ePulse Intranet Site utilized
  - Published on an as needed basis
  - Many ignore – Does provide timely information
- **Continuous “Real World” Testing**
  - Phishing Test emails delivered to all employees Monthly

# User Awareness – Phishing

- Multiple solutions available for enterprise environments
- Set of 10-12 random templates with link to page to provide on the spot training when clicked (or attachment opened)
- Attempt to keep "Positive" - acknowledge successful detection
- Monthly keeps Employees aware and alert
- Failure % should trend downward with a goal of < 2%

# Information Security Training / Awareness

## Demonstrated "Positive" Results



# Questions?