MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

ADDRESSING THE CHALLENGES OF DECENTRALIZED IT IN AN ACADEMIC MEDICAL CENTER

Chuck Kesler

Chief Information Security Officer, Duke Health

Twitter: @chuck_kesler

LEARNING OBJECTIVES

- How to use risk assessments to develop a stratified approach to addressing decentralized IT challenges
- Methods for engaging decentralized IT support staff and making them advocates for the enterprise security program
- Governance strategies for driving change across decentralized IT units
- Approaches for creating flexible security controls that can address differential risks and business constraints across decentralized IT units
- Metrics for measuring and reporting on the effectiveness of security controls across decentralized IT units

WHAT IS AN ACADEMIC MEDICAL CENTER (AMC)?

- Organizationally or administratively integrated with a medical school
- Principal site for medical school's students
- Conducts human subject research with patients of the medical center
- Healthcare providers wear multiple hats – clinician, faculty, researcher

sources: Advisory Board, Association of Academic Medical Centers, JAMA

OVERVIEW OF DUKE HEALTH

Academic Entities	• School of Medicine • School of Nursing • Duke-NUS Medical School (Singapore)
Major Teaching Hospitals	• Duke University Hospital (DUH) • Duke Medicine Pavilion (DMP) • Durham VA Hospital
Community Hospitals & Outreach	• Duke Regional Hospital (Durham) • Duke Raleigh Hospital • Community & Family Medicine, Homecare & Hospice
Ambulatory (200+ clinics)	• Duke Primary Care (DPC) • Private Diagnostic Clinic (physician practice)
Partnerships	• Duke LifePoint • Duke Community Connect & MedLink • Heart Care Plus w/ WakeMed (Raleigh)

2017 Statistics

- #17 medical center in US
- #1 hospital in NC
- #7 School of Medicine in US
- #1 School of Nursing in US
- #1 PA Program in US
- #10 Physical Therapy Program in US
- 28,000 employees
- 2nd largest private employer in NC
- 68,000 inpatient stays
- 2+ million outpatient visits
- $650M+ annually in sponsored research
- $3B+ in annual revenue
- ~5M patient records

source: https://corporate.dukehealth.org/who-we-are/facts-statistics

rankings are based on the 2017-18 US News & World Report survey

DUKE'S MISSION

In *advancing health together*, we will:

- **Deliver** tomorrow's health care today
- Accelerate **discovery** and its translation
- Create **education** that is transforming
- Build healthy **communities**
- Connect with the **world** to improve health globally

Accomplishing this mission requires:

- Generating and managing tremendous amounts of data
- Pervasively sharing data across systems and organizations

TYPES OF SENSITIVE DATA IN AMC

- Protected health information (PHI) and other PII (e.g., SSNs)
- Clinical trial data for sponsored studies (e.g., NIH, pharma)
- Research protocols and unpublished results
- Production processes (e.g., pharma)
- Financial records and transactions
- Strategic business plans (e.g., M&A)
- Student records

INFORMATION SECURITY CHALLENGES IN AN AMC

- First priority is taking care of patients
- Breakneck pace of research and innovation
- Complexity of systems and data flows
- Multiple compliance requirements (HIPAA, FISMA, FERPA, PCI, etc.)
- Significant budget constraints – need to do more with less
- **De-centralized governance and IT**

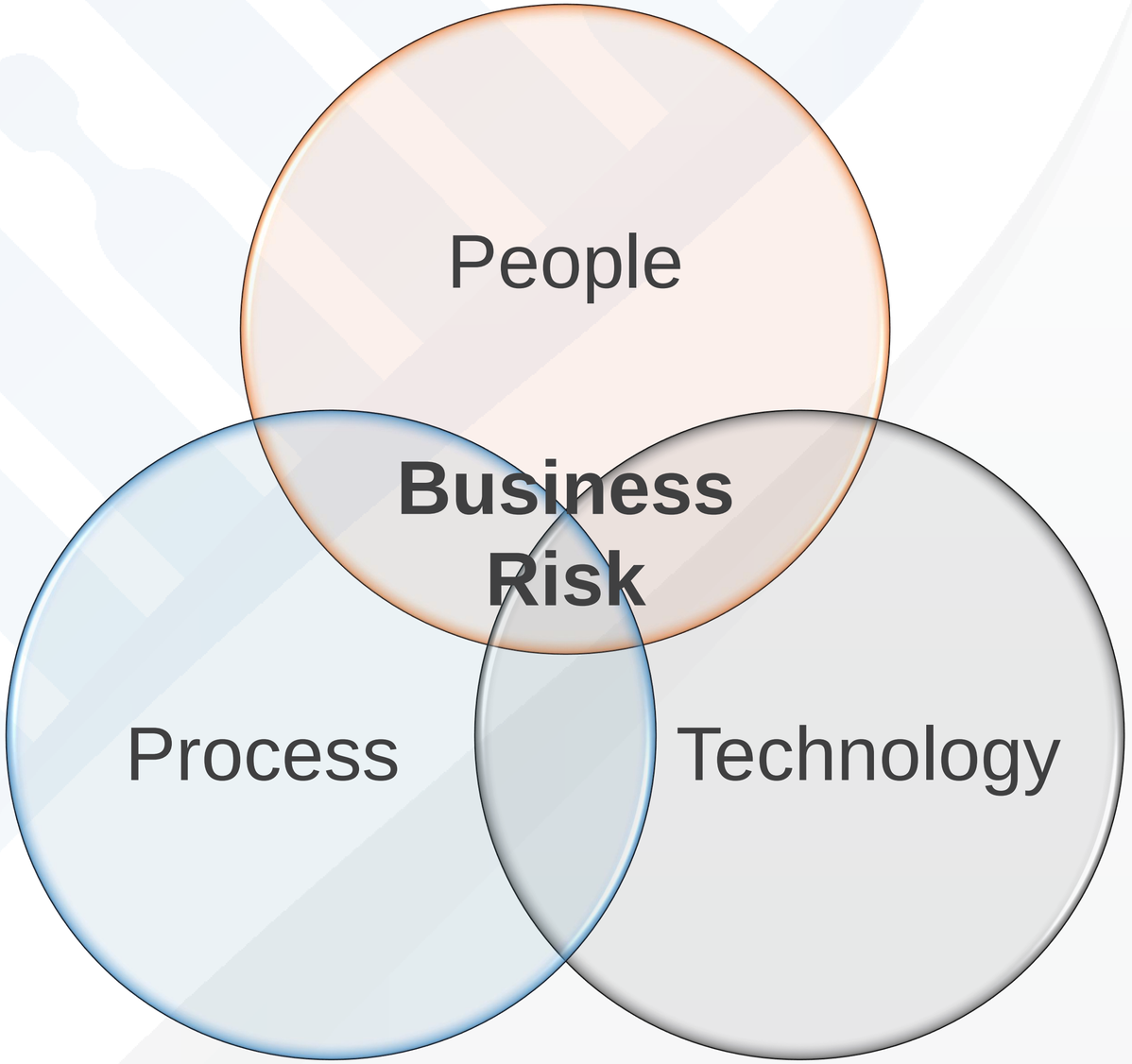
This makes it difficult to:

- *know where the data is*
- *know who has access to it*
- *know if controls are adequate*
- *maintain compliance (e.g., FISMA)*
- *detect and respond to incidents*

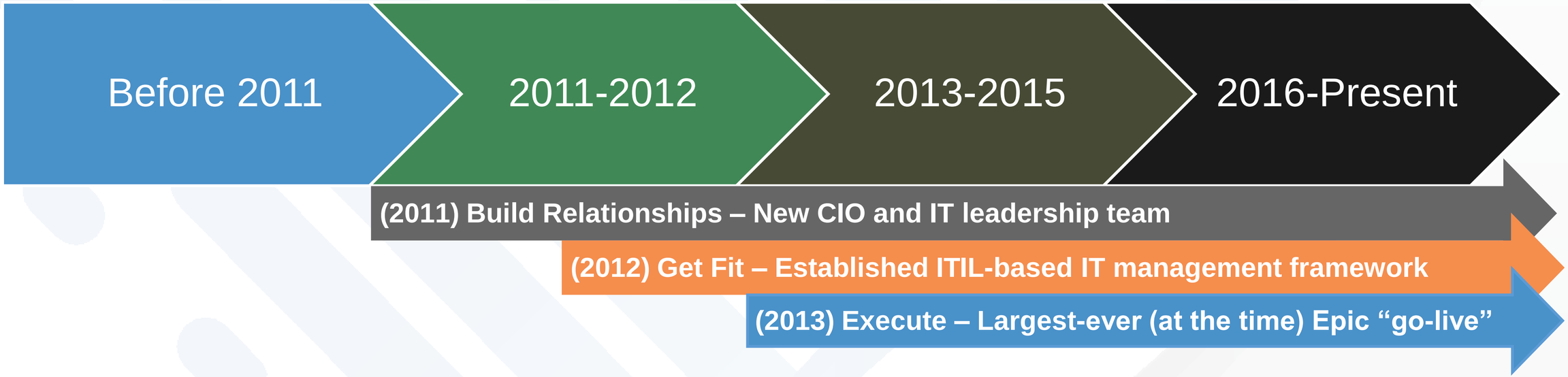
THE PROBLEM

Information security is not solely a technology problem. It's first and foremost a business risk problem.

Addressing the concerns of the affected humans and their processes are necessary for the successful implementation of technology.



THE TRANSFORMATION OF DUKE HEALTH TECHNOLOGY SERVICES



- Mostly **de-centralized**
- Each entity has its own IT shop, electronic healthcare record (EHR) system, and IT security director
- **Limited enterprise-wide** security policies and technology

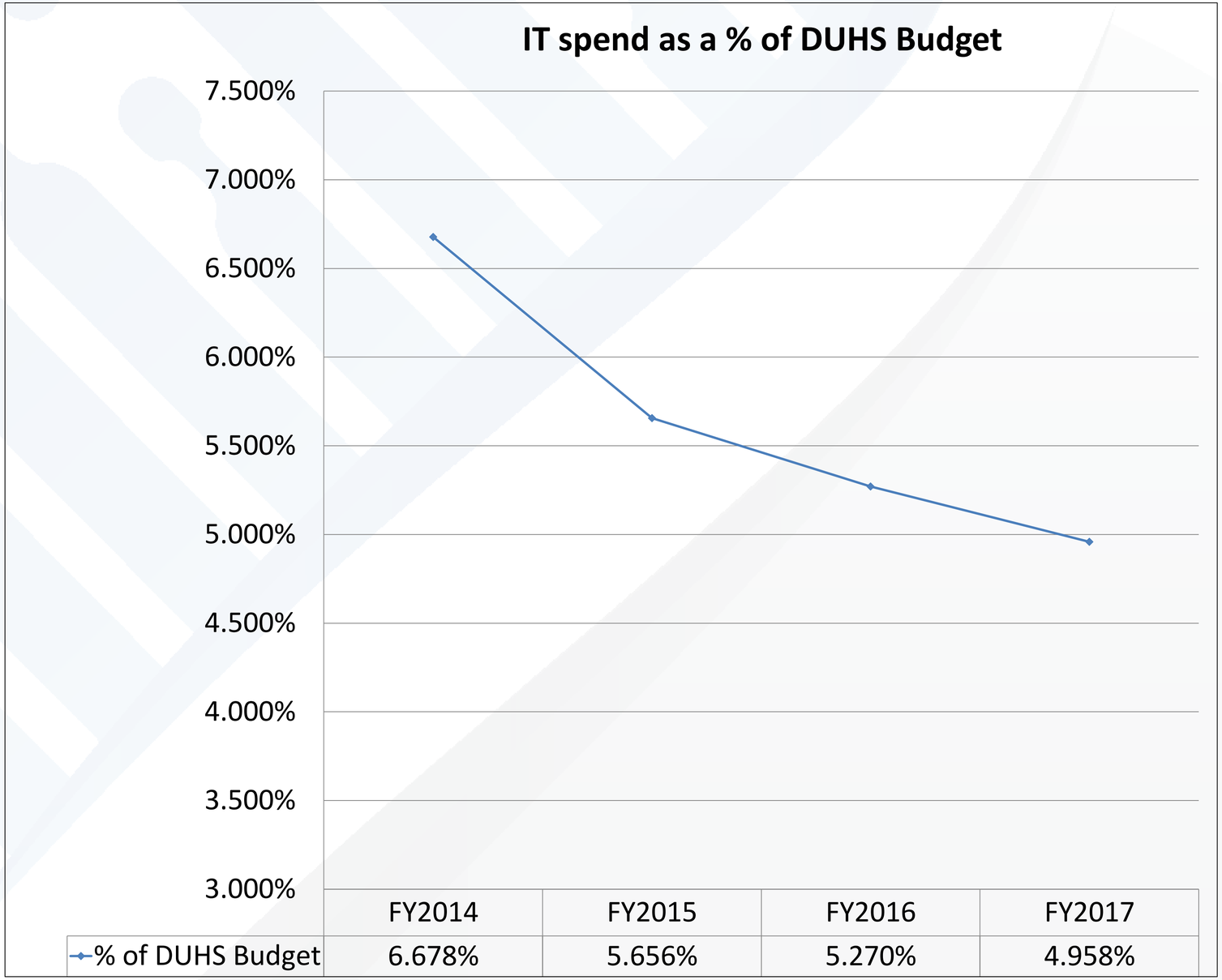
- Move to an **single enterprise-wide EHR** system (Epic)
- Consolidated most entity IT shops into DHTS (central IT)
- **Hired first CISO** and centralized authority for information security

- **Mostly centralized** w/ 800+ IT staff in DHTS
- Still a number of de-centralized IT units, ranging in size from 1-2 people to 200+
- Focused on building **enterprise controls** and policies for infosec

- Recognized risks around inconsistent controls in some de-centralized IT units
- Risk analysis driving further consolidation of some, but not all, units
- **Everyone must play by the same rules!**

HOW WE'VE DONE

- Centralized IT model largely has been viewed as a success
- Established a track record of delivering large, complex IT projects
- IT spend as a % of operating budget decreasing while services delivered were increased
- Trust levels with executive leadership dramatically increased
- Security receiving board-level attention with quarterly reports to the Audit Committee



CHALLENGES

- Centralized IT excels at providing enterprise-wide services at scale
- But some physicians, nurses, and researchers may have unique needs not suited for enterprise solutions
- De-centralized IT can fill these gaps, but also create risk if not managed like enterprise systems
- In 2016, we had 52 de-centralized IT units, and audits were identifying control gaps
  - Most units < 5 IT staff
  - A few had 10-20 IT staff
  - One had 200+ IT staff

THE CHALLENGE: WE DON'T KNOW WHAT WE DON'T KNOW

- Limited visibility into de-centralized IT units
  - Didn't know what systems and data they had
  - Some behind firewalls and couldn't be easily scanned
  - Required to use our endpoint management and security agents
  - But relied upon the honor system for compliance (e.g., patching)
  - Point-in-time audits showed gaps
- How do we quickly get a handle on 52 units?
  - Developed a phased approach
  - Phase 1: assess inherent risk – not quality of controls – in all units
  - Phase 2: assess quality of controls in riskiest units from phase 1

PHASE 1 RISK ASSESSMENT METHODOLOGY: STRATIFICATION

High	Clinical units with PHI and non-DHTS support
Moderate	Basic science units with non-DHTS support
Low	Clinical and basic science units with DHTS support

PHASE 1 RISK ASSESSMENT METHODOLOGY: DRIVERS

- Number of:
  - Users
  - Research protocols
  - Clinical applications with PHI
  - Research applications with PHI
  - Servers in non-data center locations
- Other factors:
  - Fragmentation of IT Support
  - Existence of BYOD/self-managed devices
  - Unit managed the computing infrastructure for an outside entity
  - Part or all of hosting infrastructure in the cloud

PHASE 1 RISK ASSESSMENT: RESULTS

Analysis

- Data loaded and analyzed in our eGRC system (Archer)
- Added systems that weren't already in our CMDB (ServiceNow)
- Scored all units based on a weighted scale

Outcome

- Identified 12 units as having the highest inherent risk
- Leadership decided to consolidate the largest and riskiest unit
- The remaining 11 units were moved to the phase 2 assessment

PHASE 2 RISK ASSESSMENT METHODOLOGY

- Controls assessed for each high risk unit
  - Hardware inventory
  - Configuration management for laptops, workstations, and servers
  - Vulnerability management (e.g., patching)
  - Physical security
  - Third party management
  - Data stored outside of Duke Health's control
  - Application controls (e.g., account management, logging)
  - Research Data Security Plans (RDSP)

- Controls rated on a three point scale
  - Effective, needs improvement, ineffective

PHASE 2 OUTCOME

- Data loaded and analyzed in our eGRC system (Archer)
- Added systems that weren’t already in our inventory to the CMDB (ServiceNow)
- Findings added to our risk register (Archer)
- Prioritized units based on risk
  - 3 high, 5 moderate, 3 low

THE CONSOLIDATION DILEMMA

- Some, but not all, decentralized IT units present considerable risk
- We could force consolidation, but... do we want to?
- Can we accomplish the same goals can be achieved without consolidation?
- Maybe we just need commitment that everyone plays by the same rules!

TO CONSOLIDATE... OR NOT TO CONSOLIDATE?

- Our centralized IT strategy is to provide a range of IT service options that offer ***value***
  - Risk reduction
  - Same or lower all-in costs due to scale
  - Willingness to listen and adapt
  - Commitment to be more responsive than in the past
  - Include them in governance processes
  - Be reasonable, and not just take the “ivory tower” approach to security

- In the end, ***cooperation and partnership*** prevails
  - Two high risk units embrace consolidation
  - One high risk unit hires new IT director that commits to DHTS partnership
  - Other medium and low risk units see value and ask DHTS to take over their IT

TRUST, BUT VERIFY

- Visibility & accountability: quarterly per-unit metrics delivered to **service owners and leadership**
- Highlight areas of key risks, e.g.
  - Devices w/o management agents
  - Devices not being scanned
  - Devices not being patched
- Red/yellow/green color coding to draw attention to areas of concern, and areas where things are going well
- Trending information to show how current performance compares to past quarters
- **Proven to drive change!**

CY 2017 Q3 Results

Total Devices	BigFix Not Installed	Scan Not Current	Vulnerability Average	Vulnerability Count
19	0	0	0.5	9
29	0	5	0.0	0
37	0	0	0.0	0
87	0	1	0.7	56
162	0	45	0.5	59
78	0	1	0.2	16
79	0	2	6.7	513
124	8	7	0.9	108
21	0	0	0.0	0
8	0	0	0.0	0
53	1	3	0.2	12

FUTURE PLANS

- **More engagement with IT staff**
  - Recently created Program Manager for Outreach, Education, and Awareness role
  - IT Security Academy (program started at Duke University)
  - Security Concierges and Ambassadors

- **Automate compliance monitoring**
  - Current approach requires manual data gathering and analysis
  - Further leveraging existing tools (e.g., ServiceNow, Splunk)

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Chuck Kesler

Chief Information Security Officer, Duke Health

Twitter: @chuck_kesler