Mary Dickerson
Assistant Vice President/Assistant Vice Chancellor, IT Security
Chief Information Security Officer
University of Houston | University of Houston System
mdickerson@UH.EDU
Overview

• Putting it all in Context:
  ➢ What is UHS?
  ➢ How does UHS “do” Cyber?

• Making Sense of the Madness
  ➢ Elements of an Effective Security Program
  ➢ Assessing Your Program
  ➢ Managing a Key Risk – Data!

• SB 944
UNIVERSITY of HOUSTON SYSTEM

University of Houston  
UH Downtown  
UH Clear Lake  
UH Victoria

- Five regional teaching centers & branch campuses
- Houston Public Media
- UH System Administration

Total FTE: 9,837

FTE By University:
- UH – 6,652
- UHD – 1,325
- UHCL – 1,238
- UHV – 552

UH System - 70
Mission

The University of Houston System provides, through the complementary missions of its four universities, access to comprehensive higher education programs and services to the diverse community of students in the Houston metropolitan area and beyond. The UH System's research and scholarship are globally significant, nationally competitive, and serve as an engine for economic development, while its public service activities enhance the quality of life in the region.

- $1.38 billion Annual budget
- 68,000 Students (approx.)
- 14,500+ Degrees awarded annually
- $135 million In research expenditures
Welcome to the University of Houston

- 15 colleges
- 7 administrative divisions
- 42,000+ students
- 2,300+ faculty

- 120 Undergraduate Majors/Minors
- 139 Masters Degrees
- 54 Doctoral Degrees
- 25 Research Centers
We Have **Everything**!
A few of the things that keep an Information Security Officer awake at night

- How much protection does our information need?
- Are we doing enough to protect it?
- How do we balance risk and cost?
- Where do we keep our sensitive information?
- What kinds of information do we have?
- Does everyone know what he or she has to do?
- Do they understand WHY?
Security expert

What competitors think I do...

What my mother thinks I do...

What the society thinks I do...

What my children think I do...

What my customers think I do

What I really do :)
UHS Information Security Team Profile

- UHS CIO
- UH CIO
- UHCL CIO
- UHD CIO
- UHV CIO

**EXECUTIVE ADMIN**
- CIS0
- UH ISO
- UHCL ISO
- UHD ISO
- UHV ISO

**MANAGERS (3)**
- ENTERPRISE IT SECURITY ANALYSTS
  - LEVEL 3 (4), LEVEL 2 (1), LEVEL 1 (3)

**STUDENT WORKERS (4)**
- AWARENESS SPECIALIST
The UHS Information Security program is funded solely through System Service Charge (SSC) with direct flow to Program cost centers.

The SSC allocation is 6% of each UHS university’s IT budget and covers all Program tools, costs and initiatives.
Key Centralization Initiatives (as defined by Audit)

1. **Centralized UHS Information Security Program**
   - Info Security Program Advisory Council
   - ISO local at each UHS university
   - CISO to provide backup for ISOs
   - UHS-wide information security standards
   - Centralized budgeting for Information Security

2. **Comprehensive UHS Vulnerability-Scanning program**
   - Internal scanning
   - Web Application scanning
   - Established remediation protocols
   - SDLC requirements to include scanning

3. **3rd Party Hosted Services – Assessment Process and Controls**
   - Include ongoing assessments
4. Centralized SIEM for UHS

5. Comprehensive UHS Incident Response Plan
   • Defined procedures at UHS and local campuses
   • Testing and documentation
   • Escalation processes defined

6. UHS Standardized Risk Assessment Process
   • Critical systems
   • Departmental
   • Compliance-specific
   • Comprehensive program

7. UHS Security Operations Center (SOC)
Making Sense of the Madness
• [http://www.texascisocouncil.org](http://www.texascisocouncil.org)
  • Information Security Program Essentials
    • The 37 Page Guide is a Back to Basics Approach for Information Security Management and is a “Step In” Simplified Framework
Assessing Your Program

- http://www.cyberhouston.org
  - Cybersecurity Preparedness Assessment
  - Cybersecurity for the Board of Directors
Managing a Key Risk: Data!!!

- Know What Data You Have and Where It Is
  - Who are the Business Owners?
  - What are the Compliance Requirements?
  - Standardize Storage Locations & Protect
Texas Senate Bill 944 (86R)

Key Components:
- Defines specific additional Public Information Act Requirements related to personal devices
- Enforced Record Retention Requirements
Types of Correspondence

- Non-Business Correspondence
- Transitory Correspondence
- Agency Business Records

Policy Example:

http://uhsystem.edu/compliance-thics/_docs/sam/07/7a6.pdf
Transitory Correspondence

- Transitory correspondence is not essential to the fulfillment of the statutory obligations or to the documentation of agency functions.

- Examples of transitory correspondence are:
  1. Routine messages
  2. Telephone message notifications
  3. Notices about internal meetings or events
  4. Routing slips
  5. Incoming letters or memoranda of transmittal that add nothing of substance to enclosures
References:

Text Messages Capturing and Retaining:
https://www.tsl.texas.gov/slrm/blog/2018/04/faq-so-text-messages-can-be-records-how-do-we-capture-and-retain-them/

Texting Allowed But Only of a Transitory Nature (Scroll down to this subheading at the following link):

Examples from the site – even though these are from Washington State, they parallel the Texas state requirements:

City of Shoreline Policy - Establishes that all text messages should only be used to send messages of "transitory" nature. ***Provides specific examples of texts that are allowed and texts that are not allowed***
http://mrsc.org/getmedia/65b592cf-5d0a-4390-9044-566c4d97d4d4/s55txtmsgpol.aspx
City of Kent Personnel Policy – Text Messaging Policy – Draws a distinction between “transitory” and “non-transitory” texts and provides that non-transitory texts should not be sent. It also provides procedures to follow when a public records request for texts is received depending on whether the text is on a city-owned or a personal cell phone.

http://mrsc.org/getmedia/1ecb9186-e2be-4445-958f-2a4aa217f46b/k44text.aspx