The Office of the Chief Information Security Officer (OCISO)

Department of Privacy and Security

Bring Your Own Device (BYOD) in the Enterprise

UTPA
THE UNIVERSITY OF TEXAS-PAN AMERICAN™

Joe Voje – CISO
UT - Pan American

Honors B.S.
Oregon State University

M.S. (Honors)
Capitol College

Certifications
- CISSP-ISSEP
- C|CISO
- Certified Ethical Hacker
- CCNA Security
- ITIL

Former Naval Officer

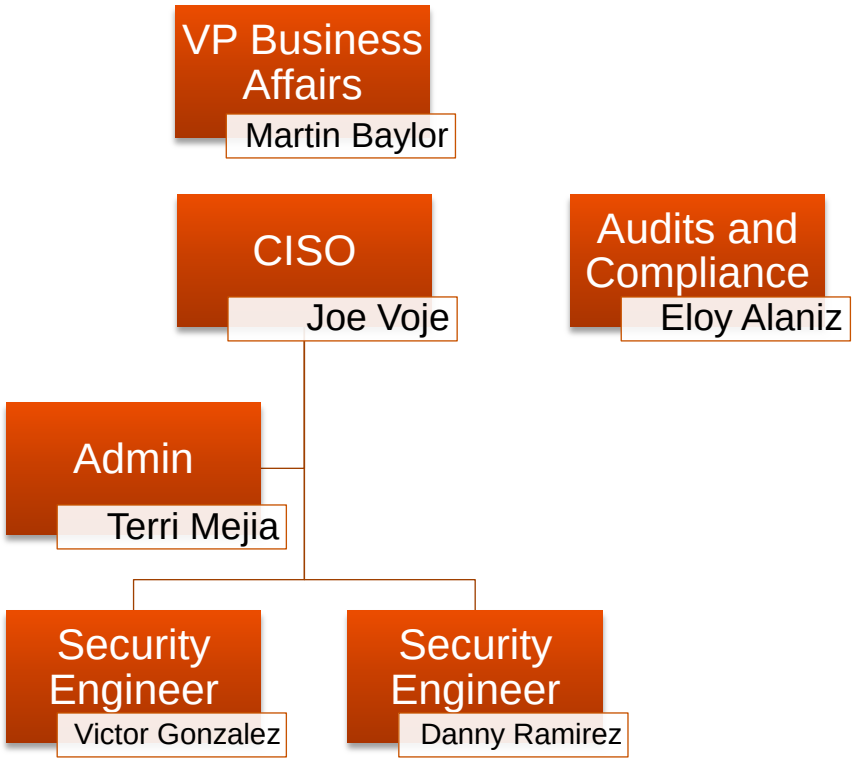
Cyber Security Experience
- Federal Government
- Financial Sector
- Energy Sector
- Research / IP Sector
- Consultant

Avid sailor and motorcyclist
- S/V Rondelet and Haj

Two superpowers

"Yeah - we used to call them cell phones."

OCISO Organizational Structure



UT – Pan American

OVERVIEW

The University of Texas-Pan American, a Hispanic serving institution, is in the middle of one of the fastest growing areas in the nation, the southern tip of Texas known as the Rio Grande Valley. UTPA is located in Edinburg, Texas, approximately 10 miles north of the US/Mexico border and 75 miles northwest of South Padre Island. UTPA provides an affordable education and global opportunities with a choice of 54 bachelor's, 55 master's, three doctoral, and two cooperative doctoral programs within 7 colleges.

FAST FACTS

Fall 2013

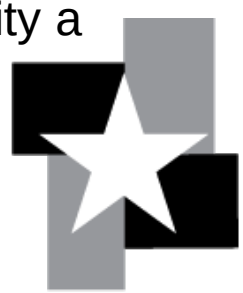
Undergraduate Student Enrollment	17,602
Graduate Student Enrollment	2,451
Total Enrollment	20,053
Total Faculty (Fall 2012)	836
Total Staff (Fall 2012)	1,136

Consumerization of Information Technology

Past. – Corporations provided individuals with expensive, cutting edge computing and mobile telecommunication devices (including high speed Internet).

Present! – Corporations and individuals are mostly on par. Individuals own their personal broadband capable devices equal to or better than corporate assets. Individuals want access to corporate services and information from a single device.

Future? Except in extreme security environments corporations may expect users to provide all of their own technology. Advances in data segregation and mobile device management are making this possibility a reality.



Intro to BYOD & Problem Scope

What is a device?

- Laptop, mobile phone, tablet, external storage media, camera, ?
- What about cloud services?

Who owns information?

- Very complicated in college and university settings
- Mine, yours, ours…

Who owns the device?

- BYOD would indicate the user does, but the device doesn't care
- What if the company pays or does not pay a stipend?

Privacy vs. Protection?

- Individual privacy and ownership issues can cloud how data is protected and which controls are used (e.g. PIN and wipe)

BYOD Policy

Put it in writing!

- Allow it / prohibit it / make exceptions
- Don’t put anything in writing that can’t be enforced by technical controls
- You will get push back
  - Screen locks
  - PIN complexity
  - Data wiping / Data segregation
  - Failed login attempts
  - What happens at separation from the organization

Train your employees on your policy and mobile device security in general

Sell it as a service

- Lost device location
- Personal data protection
- Job protection

Mobile Device Management

It's two in the morning, do you know where your data access points are…

- Quietly resting on night stands charging for the day to come…
- Wedged in the seat of a cab left behind on the way to a one night stand…
- Camping out in the airport stranded by a missed connection…
- Some are really camping…
- Entertaining insomnia inflicted security professionals preparing for TACUA briefs…
- Heck, I have no idea what my device does after I go to sleep…

Should I care?

Mobile Device Management

The correct answer is… Yes. Mobile devices provide access to some of your most critical communications and data.

Email, docs, text, apps… angry birds

Most devices have a mix of personal and professional data.

MDM solutions help segregate data into containers to protect data if the device is lost or stolen or the employee/employer relationship changes.

Email segregation is easy, but…

Challenges exist

- Photos (ever take a photo of a whiteboard)
- Malicious apps

Mobile Device Management

On the cheap…but less elegant

Gain control of your devices through Microsoft Exchange (ActiveSync).

- Enforce passwords / PINs
- Remotely wipe lost or stolen devices
- Wipe devices that are being attacked through brute force
- Communicate with the device

What devices can you control with MS Exchange?

- iOS (Apple) iPads, iPhones, iPod Touch
- Windows phones
- Android devices
- RIM (Blackberry)

Mobile Device Management

More elegant solutions are provided by a number of vendors.

True MDM solutions account for:

- Segregation of personal and professional data
- Can safeguard information beyond email
- May add encryption and Data Loss Prevention capabilities

Examples of vendors include:

- Mobile Iron
- AirWatch
- Sophos

Supervisor Responsibilities

As supervisors you have additional responsibilities beyond those of the traditional consumer of information resources.

You may have responsibility for the physical accounting of computing resources such as desktops, laptops, and tablets.

But you also have responsibility for the proper handling of information by the employees you supervise. Almost all supervisors will handle sensitive Personally Identifiable Information (PII), such as employee ID numbers, student ID numbers, social security numbers, etc.

To maintain the public trust and the trust of our students and employees it is imperative that we handle this information in a secure manner. To help train our faculty and staff in the threats to information resources we ask that you ensure that your employees take the Information Security Training each year.

Protecting Information

The first step towards protecting sensitive information in your area of responsibility is to understand the type of data you have within your department or division.

Next you need to understand:

- How it is used
- Where it is stored (individual computer, file share, or encrypted USB drive)
- Who needs access to it (employees, outside collaborators, the public)

Last you need to understand the regulatory environment you are working under. At the University information you are handling may fall into one or more mandatory regulatory environments, such at FERPA, PCI, GLBA and a host of other regulations.

For help determining your environment contact the OCISO.

State, UT System & UTPA Rules

In addition to the Federal regulatory environment, The State of Texas, The University of Texas System and The University of Texas – Pan American have specific and supporting rules to protect information resources and data.

Texas Administrative Code (TAC) Title 1 Part 10 Chapter 202 sets standards for Information Security for Institutions of Higher Education and State Agencies.

The University of Texas System Administration Policy – UTS165 – defines UT System Information Resource Use and Security Policy.

HOP 8.9.1 and HOP 8.9.2 in addition to the UTPA Security Manual provide policy and procedures for security controls at UTPA.

We're from the Government…

Helpful documents to craft your institutional BYOD / MDM strategy:

Guidelines for Managing and Securing Mobile Devices in the Enterprise
http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

Security and Privacy Controls for Federal Information Systems & Organizations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

The White House / Digital Government / Bring Your Own Device
http://www.whitehouse.gov/digitalgov/bring-your-own-device

BYOD: The elements of getting it right the first time
http://gcn.com/articles/2013/03/29/byod-getting-it-right-the-first-time.aspx

Questions or 404 errors

Contact Information

The University of Texas – Pan American

Joe Voje
Chief Information Security Officer
956.665.7823
infosecurity@utpa.edu

http://www.utpa.edu/infosecurity