University of San Diego

Health Care Cyber Security

How to Mitigate Threats and Manage Risk Through Human Factors

Welcome!

- This session is being recorded. We will send you a link to the recording after the session.
- There will be time for Q&A at the end. You can enter your questions in the chat pane at any time
- If you have questions, please type them into the chat pane in your AnyMeeting app

University of San Diego

About University of San Diego

- Catholic institution founded more than 60 years ago
- Ranked in the top 100 Online Graduate Education programs by *U.S. News & World Report.*
- Selected as a designated Ashoka *Change*maker Campus
- Hahn School of Nursing and Health Science top ranked in Research & Clinical Practice
- Now offering a number of professional graduate degrees in an online format, including an M.S. in Health Care Informatics

BEST U.S.News & World Report RANKINGS

WASC Senior College and University Commission

University of San Diego

About Today's Presenter

Jonathan Mack, Ph.D.

Clinical Associate Professor

Program Coordinator, Graduate Program in Health Care Informatics (M.S.)

And Nursing Informatics (MSN)

University of San Diego

Webinar Objectives

In the next hour, you will learn:

- The cyber risks that currently exist in the health care environment
- What cyber hygiene is, and how human factors is critical for success
- Programs and techniques that you can put in place to manage ongoing cyber threats

University of San Diego

What is Cyber Hygiene?

Cyber hygiene is a term that describes a set of practices, measures, and/or actions a user can take to protect: a work station(PC) , computer networks, and mobile devices from cyber attacks.

Cyber Hygiene is considered the **human factor** side of cyber security as it focuses on the human element to protecting systems

A Cyber Primer: Common Terms

Cyber Security:	focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.
Cyber Hygiene:	Actions that individuals carry out to protect work stations, networks and devices. The human factor in cyber security
Malware:	Any type of code or software that performs an unauthorized function
Phishing:	Software that deceives an individual into providing information. Usually occurs in the form of emails or attachments
Blacklist:	A list of entities that are considered risk to electronically contact
White list:	a List of organizations or web sites that are considered safe to contact
Penetration testing:	a Method organizations use to assess for system vulnerabilities
Data Breach:	Unintentional release of information to unauthorized individuals or entities
Firewalls:	Cyber Software that acts as firs line of defense on a network

University of San Diego

What is Malware?

Malware is short for malicious software – a general term that encompasses a variety of online threats including:

- **Spyware** -Used to track your internet activity and steal data like credit cards
- **Viruses** - Replicate themselves and are passed to other users
- **Worms** - Same as Viruses but does not require human action to spread
- **Trojans** - Disguised as safe programs and user installs allowing hacker to steal data
- **Adware** -isplays marketing information in Banners collects user data usually not malicious
- **Ransomware** -Encrypted software blocking access to owner user of the device and their data

University of San Diego

Why is Health Care a Cyber Target?

- Health Care organizations did not have a significant web presence (or clinical data was not accessible) until after 2010 when Meaningful use program was implemented.
- Expanded use of wireless devices and mobile smartphones to access data
- Health Care data is more valuable on the dark web than credit card data.
- Health care data provides more complete data for creating Fraudulent transactions. Credit card numbers can change after they are reported stolen but social security, birth dates and home address usually do not.
- Recent ransomware hacks set a precedence in that health care organizations paid ransom demands to gain back data access.

University of San Diego

What Makes Health Care a Higher Risk Industry?

- The health care industry is playing catch up with other industries that use system wide data management. Health Care organizations have not kept pace with the vulnerabilities that new technology presents.
- Health Care organizations have not trained staff to manage risks and use simple Cyber Hygiene techniques.
- Overall health care organizations do not have the expertise to manage cyber threats.

University of San Diego

Types of Health Care Breaches

Most Breeches in Health Care Data remain unintentional. Unintentional includes the following:

- Lost laptops with clinical data
- Lost USB drives with clinical data
- Hard copy data not shredded properly and sent to trash
- Spreadsheets with clinical data sent to unintended individuals
- Faxed data sent to unintended recipients
- Patient portal release of data not intended for that patient

How Do Hackers Access Health Care Systems?

Cyber attacks can happen in phases:

1. Cyber attacker identifies an organizations network.
2. Cyber attacker searches for vulnerabilities in the outward facing systems that can be exploited. The attacker may run a port scanner against the network to discover ports that were mistakenly left open or the attacker could run a vulnerability scanner against the target network to try to identify old vulnerabilities that the victim failed to patch.
3. Cyber attacker may infect perimeter devices and analyze outbound network traffic with software called a “packet sniffer” in order to capture trusted user credentials.

University of San Diego

How Do Hackers Access Health Care Systems?

4. Cyber attacker can steal user credentials by generating a realistic fake website and tricking the user into entering their credentials.
5. Cyber attackers may send phishing emails to staff in an attempt to trick the employees into revealing specific information. Phishing emails are scam emails that either contain malware that allows attackers into a system by installing a virus, Trojan, etc., or they trick the user into responding to the email with their system credentials.

The Most Common Portal of Entry for Cyber Attacks

Phishing emails remain the most effective method for introducing a software vector (malware) into a health care computer network.

- In some cases, the emails appear legitimate because the hackers obtain information they stole from other sources that are recognizable by the target staff
- Careless internet browsing, including accessing high risk web sites

University of San Diego

Data Breaches Through Cyber Attacks

Ransomware

- Ransomware is a type of malware that limits or eliminates access to a users systems by encrypting a users data
- There are approximately 70 different types of ransomware
- Organizations often discover they've been infected with malware only after workers start complaining that they can't access files on a shared server.

University of San Diego

Ransomware

- Most common method of infection to PCs and Networks is through infected spam email (with an attached document) that directs readers to enable macros or clicking on a link
- Expect such attacks to increase, says James Scott, senior fellow at the Institute for Critical Infrastructure Security (ICIT), which recently released a report on the ransom ware threat to organizations in critical infrastructure sectors.

"Hospitals are an easy target for many reasons. Employees typically lack cyber hygiene training and their technology landscape, in most cases, is eerily absent of layered security centric protocols." – James Scott

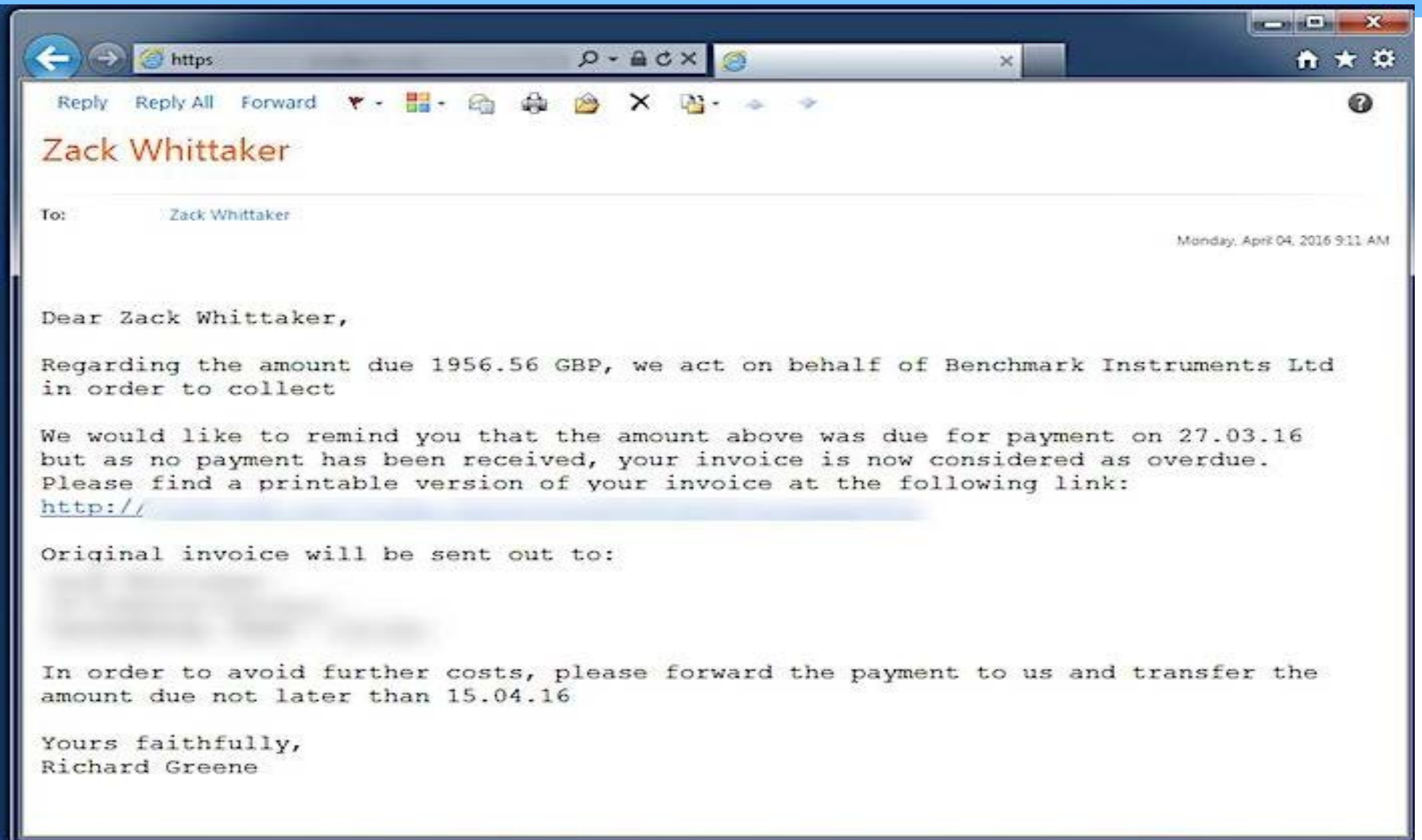
University of San Diego

HCOs Recently Hit by Cyber Attacks (Ransomware)

- Kansas Heart Hospital May 18, 2016
  **Agreed to pay the ransom however the Hackers did not release data and asked for additional ransom*
- MedStar Health, which operates 10 hospitals and more than 250 outpatient clinics in the Maryland/Washington, DC area
- Kentucky Methodist Hospital
- Prime Health Inc., owner of
  - Chino Valley Medical Center, California
  - Desert Valley Hospital, California
  - Alvarado Medical Center, San Diego, California
- Hollywood Presbyterian Medical Centre in Los Angeles
  Paid $17,000 to get access back

University of San Diego

Example of Ransomware Phishing



Reply Reply All Forward

Zack Whittaker

To: Zack Whittaker

Monday, April 04, 2016 9:11 AM

Dear Zack Whittaker,

Regarding the amount due 1956.56 GBP, we act on behalf of Benchmark Instruments Ltd in order to collect

We would like to remind you that the amount above was due for payment on 27.03.16 but as no payment has been received, your invoice is now considered as overdue. Please find a printable version of your invoice at the following link:
http://

Original invoice will be sent out to:

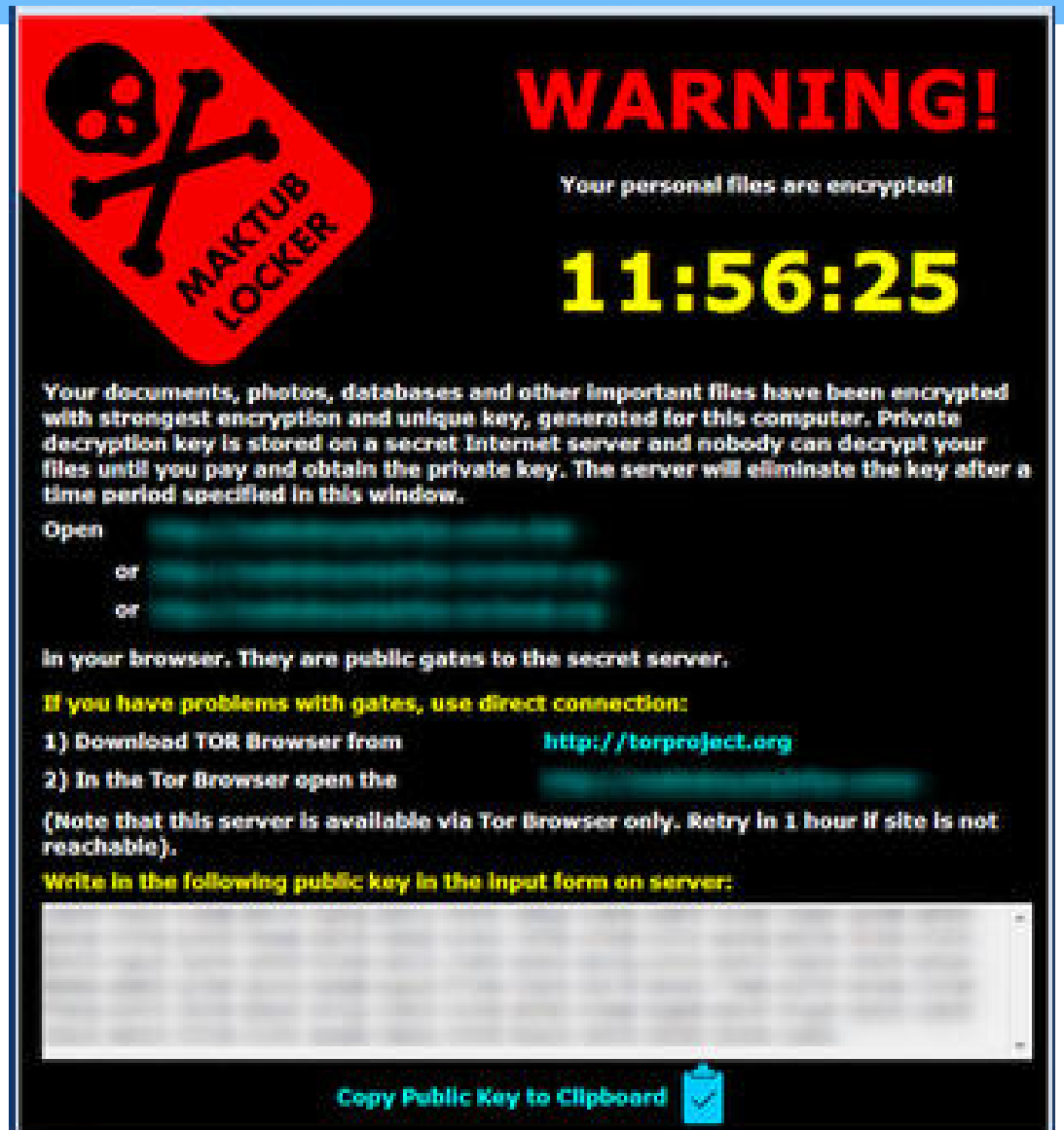
In order to avoid further costs, please forward the payment to us and transfer the amount due not later than 15.04.16

Yours faithfully,
Richard Greene

By Zack Whittaker for Zero Day, April 7, 2016

Example of Ransomware Threat Notice

Example of Screen Lock Warning with Ransomware



How to Recognize a Computer Virus Infection

- Some typical symptoms of an infected computer include:
- System will not start normally (e.g., “blue screen of death”)
- System repeatedly crashes for no obvious reason
- Internet browser goes to unwanted web pages
- Anti-virus software appears not to be working
- Many unwanted advertisements pop up on the screen
- The user cannot control the mouse/pointer
- Dialogue boxes directing user to pay to releases data (Ransomware)

University of San Diego

Infected with Ransomware? Follow These Steps

- Shut down networks and infected systems (train staff to physically disconnect an infected workstation)
- Disable Wi Fi and Bluetooth to prevent malware from spreading
- Instruct staff to remove any USB or external drives and quarantine them. This is to stop them from being infected and if they are infected prevent then from transmitting the malware.
- Try to discover what type of ransom ware has infected your systems
- Activate appropriate down time procedures/disaster response plan
- Notify in-house Legal and Risk management
- Contact Homeland Security, Local FBI office, and or local law enforcement

University of San Diego

Applying Cyber Hygiene to Reduce Threats

- Think of Cyber Hygiene as the human side of threat mitigation with simple steps that are easily taught
- Hand Hygiene Programs can act as templates for Cyber Hygiene Prevention Programs.
- The Human element of cyber hygiene has shown to impact the greatest in reducing cyber threats
- Training and ongoing assessment is key component

Hand Hygiene Saves Lives

University of San Diego

Organizational Strategy for Reducing Threats

- Inventory and control purchase for all devices and software
- Develop and manage secure configurations for all devices.
- Conduct continuous (automated) vulnerability assessment and remediation.
- Actively manage and control the use of administrative privileges.
- Develop and maintain a cyber plan with a disaster recovery plan (to include down time procedures).
- Carry out ongoing threat assessment and compliance monitoring for basic hygiene .
- Make sure your disaster plan has expertise contracted to assist with cyber remediation.
- Scheduled meetings between I.T and Clinical

University of San Diego

**This is a brief list of cyber hygiene methods and does not include all possible methods to reduce cyber threats*

Staff Level Cyber Hygiene

- Make cyber hygiene and cyber security a priority, as important as National Patient Safety Goals(the Joint Commission 2016).
- Make Cyber hygiene part of all new employee orientation and annual staff competencies.
- Train networks which includes initial actions to be taken when a station is infected. staff to identify possible threats to workstations, medical devices and
- Train staff to identify ongoing system vulnerabilities (phishing emails)
- Limit access to critical network areas and functions
- Limit or eliminate staff's ability to add software or peripherals

University of San Diego

**This is a brief list of cyber hygiene methods and does not include all possible methods to reduce cyber threats*

Small Practice Readiness for Cyber Security

- Use strong passwords and change them regularly (every 90 days).
- Install and Maintain Anti-Virus Software and operating system updates.
- Use a Firewall on all network connections and wireless routers.
- Control Access to Protected Health Information . Assign access based upon need.
- Control Physical Access: This includes all hardware such as USB drives, peripherals .
- Limit and control use of 3rd party software: Ensure process in place for monitoring staff's ability to add or change software.
- Limit Network Access.
- Plan for the Unexpected: Have down time plan and procedures.
- Maintain good computer habits.
- Establish a Security Culture: New employee and yearly staff competencies in cyber hygiene.
- Maintain readiness by running cyber drills just as you would for fire drills.
- Assess ongoing vulnerabilities by testing network and staff.

University of San Diego

**This is a brief list of cyber hygiene methods and does not include all possible methods to reduce cyber threats*

Consider Cyber Liability Insurance

- Cyber insurance protects organizations against civil liability claims
- Usually provides technical and legal support in the event of a cyber incident
- Provide educational services
- Provide loss claim service

University of San Diego

USD's M.S. in Health Care Informatics

- 100% online program
- 10 three-unit courses + capstone course
- Two courses per semester (back to back)
- Complete the program in 20 months (5 semesters)
- 31 academic credits with curriculum designed to prepare graduates for leadership roles in health care informatics

University of San Diego

Curriculum

Integrates health care technology, leadership & management

Technical Courses:

- Intro to Health Information Mgmt.
- Intro to Health Care Delivery Systems
- Systems Analysis & Design for Health Care Informatics
- Database Design & Knowledge Management
- Advanced Health Care Information Management

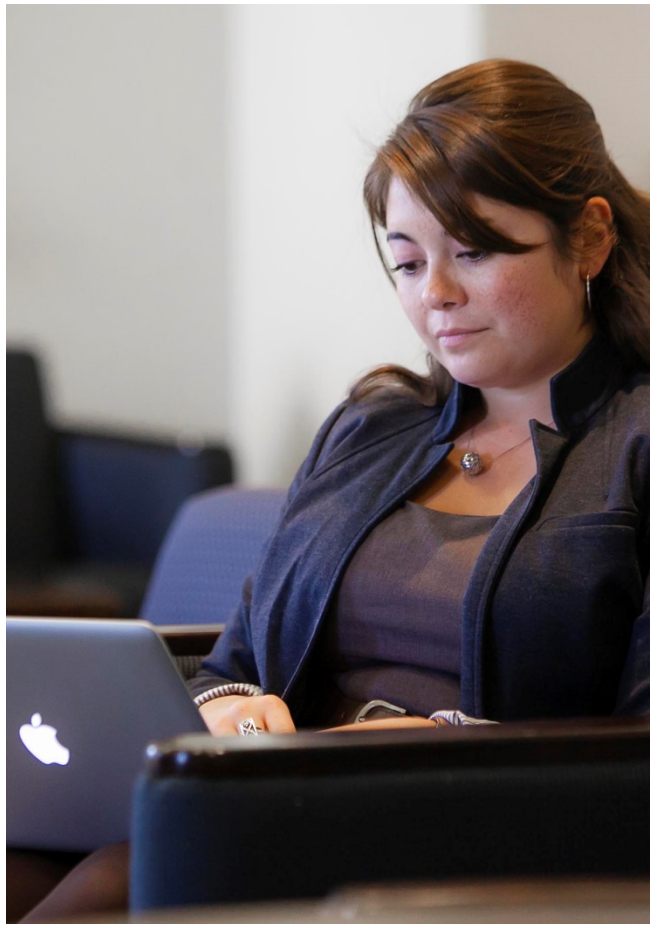
Business Management Courses:

- Health Care Leadership, Values & Social Justice
- Financial Management in Health Systems
- Management of Health Systems Care Delivery & Outcomes
- Strategic Planning & Management of Health Systems
- Statistics

University of San Diego

Online Learning

- Courses are *100% Online – available 24/7*
- Provide a flexible and convenient, yet rigorous, learning structure
- Access course content and resources anywhere with an internet connection
- Courses utilize multi-media, facilitated discussion forums, and student collaboration to create a learning community



University of San Diego

Application & Tuition

Application Fee: ***$45 – Waived for Webinar attendees!*** *(Discount Code will be sent in a follow up email)*

Tuition per unit: $925 → this is 35% less than the on campus program!

Learn more at HCInformatics.SanDiego.edu

University of San Diego

Questions?

Jonathan Mack, Ph.D.

Please use the question pane to type any questions you have for Dr. Mack

Learn more at HCInformatics.SanDiego.edu

University of San Diego

Cyber Security and Cyber Hygiene Tools

Cyber Security: A Shared Responsibility
https://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility

HHS Security Risk Assessment Tool
https://www.healthit.gov/sites/default/files/risk_assessment_user_guide_final_3_26_2014.pdf

Homeland Security
https://www.dhs.gov/topic/cybersecurity

Cyber Incidence Response
https://www.dhs.gov/cyber-incident-response

HiMSS Health Information Management and Systems Society Privacy and Security
http://www.himss.org/library/healthcare-privacy-security

Cyber Security Primer for Health care and Public Health Sector
http://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-primer.pdf

Hacking Health Care 2016
http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf

University of San Diego