CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

University of Louisville -- Lead Institution
Presenting on behalf of the team:
Dr. Andrew Wright
U of L College of Business

- Pathways Coalition
- Healthcare Track
- 13+ Schools
- Subject Matter Experts from Healthcare
- 23 Modules in Clark Open Source

DIGITAL TRANSFORMATION CENTER

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

Explorer (Badges = AI Fundamentals & Enterprise Design Thinking)

- IT Basics
- Network Foundations
- Coding
- DB Management
- Privacy/Legal Foundations and Ethics
- Security Principles & Foundations
- Cryptography
- Artificial Intelligence

Practitioner (Badges = Cloud Security, Cisco Cybersecurity and Blockchain)

- Cloud Foundations
- Network Security
- Information Security
- Cyber Threat Hunting
- Forensics
- Cognitive Computing
- Data Mining
- Blockchain

Professional (Badges = Azure IoT, RPA and Power Automate & Threat Modeling)

- DB Security
- Cloud Security
- IoT
- Post Quantum Cryptography
- Risk Analysis
- Robotic Process Automation Analysis
- Healthcare Capstone

Curricula developed as core foundational with tracks in Healthcare industry and Logistics (Labs, Datasets etc.)

Tech Industry Badges earned throughout (IBM, Microsoft, Google etc.)

Train the Trainer and Open Source modules available- please inquire

Success Coaches assigned to each student

Healthcare Cybersecurity (Certificate)
6 months/8 week courses/online instructor led—Cohorts of 35-40
First group launched Fall 2021

- **Enhancements:**
  - Logistics
  - Train the Trainer – inquire NOW
  - Cybersecurity Analyst
  - Cybersecurity Technical Specialist

PATHS to:

*Associate
*Bachelors
*Graduate Degrees
And/or
Certificates

https://bit.ly/ULWorkCyber | 502.852.3871

Healthcare and Logistics Tracks – Workforce Certificate | 04.08.22

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

Explorer (Badges = AI Fundamentals & Enterprise Design Thinking)

- **IT Basics**
- **Network Foundations**
- **Coding**
- **DB Management**
- **Privacy/Legal Foundations and Ethics**
- **Security Principles & Foundations**
- **Cryptography**
- **Artificial Intelligence**

- Non-credit, certificate and/or digital badge(s) earning
- Assume no prior experience, so included some basic/foundational modules
- Coalition members led development of content working with instructional designers
- Modules include formative and summative assessments, including:
  - Embedded knowledge checks
  - Hands-on labs
  - Case studies
- Industry focus provided through application context via data sets, case studies, etc.

Explorer
DB Management

The given dataset, covid19_subset.csv, is a subset containing daily reported covid-19 confirmed cases of the world, which is extracted from a more complete covid-19 dataset maintained by Our World in Data (https://github.com/owid/covid-19-data/tree/master/public/data). The dataset is in the csv (Comma Separated Value) file format and is partially listed below:

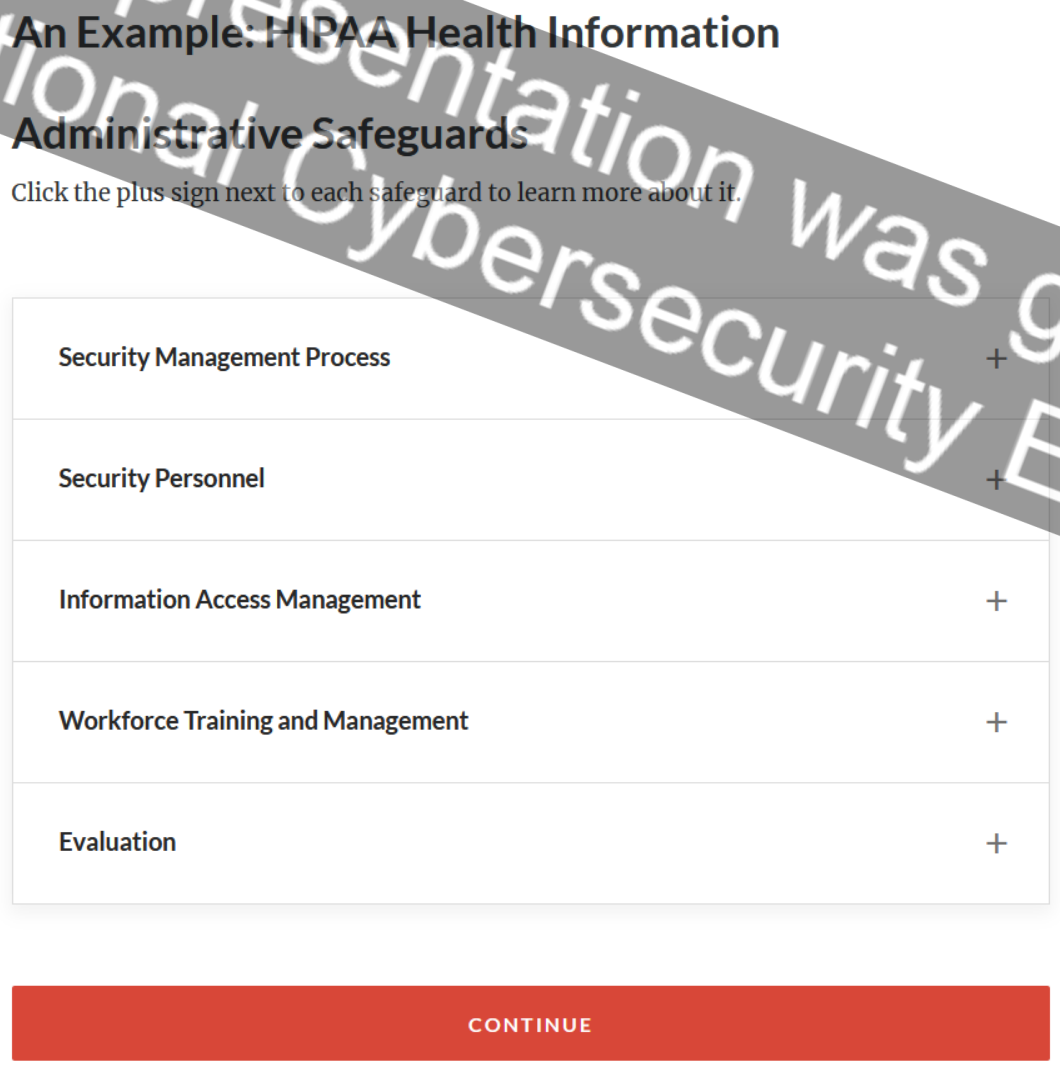
```
iso_code,continent,location,date,total_cases,new_cases
AFG,Asia,Afghanistan,2020-02-24,1,1
AFG,Asia,Afghanistan,2020-02-25,1,0
AFG,Asia,Afghanistan,2020-02-26,1,0
AFG,Asia,Afghanistan,2020-02-27,1,0
AFG,Asia,Afghanistan,2020-02-28,1,0
AFG,Asia,Afghanistan,2020-02-29,1,0
AFG,Asia,Afghanistan,2020-03-01,1,0
AFG,Asia,Afghanistan,2020-03-02,1,0
AFG,Asia,Afghanistan,2020-03-03,2,1
AFG,Asia,Afghanistan,2020-03-04,4,2
AFG,Asia,Afghanistan,2020-03-05,4,0
AFG,Asia,Afghanistan,2020-03-06,4,0
AFG,Asia,Afghanistan,2020-03-07,4,0
AFG,Asia,Afghanistan,2020-03-08,5,1
AFG,Asia,Afghanistan,2020-03-09,7,2
AFG,Asia,Afghanistan,2020-03-10,8,1
AFG,Asia,Afghanistan,2020-03-11,11,3
AFG,Asia,Afghanistan,2020-03-12,12,1
AFG,Asia,Afghanistan,2020-03-13,13,1
AFG,Asia,Afghanistan,2020-03-14,15,2
AFG,Asia,Afghanistan,2020-03-15,16,1
AFG,Asia,Afghanistan,2020-03-16,18,2
AFG,Asia,Afghanistan,2020-03-17,20,2
AFG,Asia,Afghanistan,2020-03-18,24,4
AFG,Asia,Afghanistan,2020-03-19,25,1
AFG,Asia,Afghanistan,2020-03-20,29,4
AFG,Asia,Afghanistan,2020-03-21,30,1
AFG,Asia,Afghanistan,2020-03-22,34,4
AFG,Asia,Afghanistan,2020-03-23,41,7
AFG,Asia,Afghanistan,2020-03-24,43,2
AFG,Asia,Afghanistan,2020-03-25,76,33
AFG,Asia,Afghanistan,2020-03-26,80,4
.....
```

- For most of the modules, the healthcare industry focus is readily separable so can easily replace with different industries

Your assignment is design and implement a database to store covid19_subset.csv data in your chosen database management system (DBMS), for example, MySQL. Specifically, you will follow these steps to do the project:

1. Design a database schema based on the requirements.
2. Create a SQL DDL (Data Definition Language) script to define the database schema.
3. Apply the script in step 2 to create a database in the chosen DBMS
4. Import covid19_subset.csv to the database created in step 3.
5. Run a couple of SQL queries to test your database implementation.

Explorer
Privacy/Legal Foundations and Ethics



- For most of the modules, the healthcare industry focus is readily separable so can easily replace with different industries
  - This module has deeper integration because of the complex legal environment for healthcare

Explorer
Privacy/Legal Foundations and Ethics

Homework 2 Part 1: Protected Health information (PHI)

The following 5 questions refer to the article linked below:

https://www.hipaajournal.com/considered-phi-hipaa/

Homework 2 Part 2: Data Breach Notification

In the United States, there is no single, uniform law that governs disclosure of data breaches. Instead, most states have passed piecemeal legislation with various covered elements and disclosure requirements. Companies can be (and are) held to entirely different compliance standards depending on which state an affected individual lives in. BakerHostetler maintains a comprehensive comparison of the various state data breach laws in an interactive map here:

https://www.bakerlaw.com/BreachNotificationLawMap

Summative Assignment Part 1: Premera Blue Cross Case

The following 3 questions refer to the Premera Blue Cross case linked below:

https://www.hipaajournal.com/ocr-imposes-2nd-largest-ever-hipaa-penalty-of-6-85-million-on-premera-blue-cross/

Review the case and answer the following questions.

Summative Assignment Part 2: University of Texas MD Anderson Cancer Center Case

The following 5 questions refer to the University of Texas MD Anderson Cancer Center case linked below:

https://www.hipaajournal.com/ocr-4-3-million-cmp-university-texas-md-anderson-cancer-center/

Review the case and answer the following questions.

Summative Assignment Part 3: Summary of HIPAA Violation Cases

The following 5 questions refer to the Summary of HIPAA Violation Cases and FAQs (at the bottom of the site) linked below:

https://www.hipaajournal.com/hipaa-violation-cases/

Review the site and answer the following questions.

National Security in Cyber Permeates Everything

And in light of COVID 19 we can see how what traditionally has been a local issue can explode into an issue of national security.

The cybersecurity attacks appear to be related to efforts to access clinical information regarding the treatment and research on treatments and vaccines. This by itself demonstrates the importance of medical information globally, especially in the face of a pandemic.

But if you consider how vital healthcare has been during this critical time, you could also see how efforts that disrupt healthcare computing systems can cost a great deal and bring about massive suffering.

The ransomware attacks that have hit hospitals and encrypted their data are extortion schemes that impact and negate the availability of key medical information. Think of the impact of this during a medical emergency and what it would do to the care of seriously ill patients.

This is something we must prepare for.

Why would anyone attack a hospital?

Remember, we are dealing with bad people intent on doing bad things.

Damaging the healthcare network can accomplish many things, ranging from the money you get from a ransomware attack that encrypts the data and hospital systems, making it unusable until the ransom is paid, to the disruption of public faith in the government's ability to protect people.

What are the needs for the effective operation of those systems and access to the data, and what are the risks if those fail?

To conceptualize the risks and the means by which we might be able to put up a defense, we have to look at each target and what might be the motivation to attack a target and the means by which may it be accomplished. Then you can devise a system to try and protect against those motivated attacks.

Remember, in this modern world, sensitive infrastructure systems at the hospital or a healthcare network are not just having to deal with criminals. We must also be prepared for nation-state attack that seeks to undermine the operations of our country.

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

Practitioner (Badges = Cloud Security, Cisco Cybersecurity and Blockchain)

- **Cloud Foundations**
- **Network Security**
- **Information Security**
- **Cyber Threat Hunting**
- **Forensics**
- **Cognitive Computing**
- **Data Mining**
- **Blockchain**

- The Practitioner level builds on the foundations established by Explorer
- More modules incorporating hands-on lab exercises
- During initial pilot we hosted virtual lab environments on two different platforms managed by coalition schools
  - UALR's Google Cloud-based CyberGym and UofL's hosted CyberPVE range

CyberPVE: Proxmox-based virtualization

- Proxmox Virtual Environment is a complete, open-source server management platform for enterprise virtualization

- Eight compute cluster nodes
- 224 compute threads
- 3+ TiB of RAM
- 200 TiB of NVMe distributed storage
- Can deploy over 2000 simultaneous virtual machines
- Entirely virtualized switch and routing architectures
- Each learning environment is dynamically allocated and networked

Practitioner
Network Security

Hands-On Lab Using CyberPVE

Project – MySQL Hacking with Metasploit

- This project is to understand how we can break into a target using tools such as Metasploit. Following the instructions, student will brute force logins, extract password hashes, and enumerate database users.
- *For answers, please use the accompanying word document.*

Tutorials

- Nmap: *Nmap 6: Network Exploration and Security Auditing Cookbook* by Paulino Calderón Pale.
- Metasploit: https://www.metasploit.com/
- Armitage: https://www.offensive-security.com/metasploit-unleashed/armitage-setup/
- Metasploit for Beginners - Modules, Exploits, Payloads And Shells: https://www.youtube.com/watch?v=TieUDcbk-bg&ab_channel=LoiLiangYang

Preps

- Start the **Kali (External)** and **Metasploitable** VMs.

How to use Metasploit on Kali

- First, you need to start the databases service to store all the results. Type this command on Kali: **systemctl start postgresql**.
- Second, if you're running Metasploit for the first time, you need to create a database schema. Type this command: **msfdb init**.
- Next, you start the Metasploit by typing this command: **msfconsole**.

Retrieving IP Addresses of VMs for Pentesting

Identify the IP addresses of the following VMs. You can obtain the IP addresses of each VM by manually running **ifconfig** on each VM.

a. Kali: _____
b. Metasplotable: _____

Before each exploit below, check whether you can ping the **Metasplotable**. When you cannot ping Metasplotable, login to the VM (id=**msfadmin**/pwd=**msfadmin**) and run this command: **sudo reboot.**

Tasks

References:

- https://charlesreid1.com/wiki/Metasploitable/MySQL

Practitioner
Network Security

Chesapeake NETCRAFTSMEN

White Paper

Medical Grade Network Design and Operation

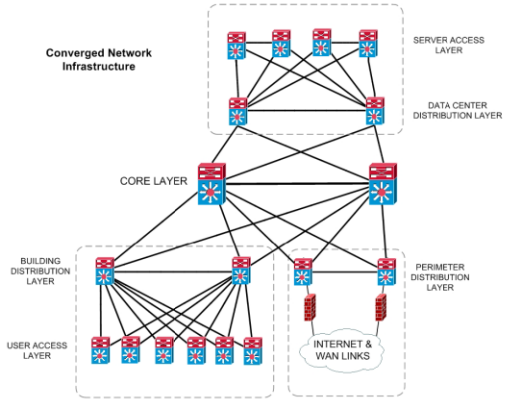
Chesapeake NetCraftsmen has been supporting our health care customers with designs and implementations of 'Medical Grade Networks'. In this whitepaper we will describe medical grade network design and discuss some of the problems that we find in real networks.

Background

Most health care organizations have an existing network infrastructure - often there are *several* physically separate networks, supporting clinical data, non-clinical data, voice, research, educational equipment, and departmental staff. For several reasons (manageability, efficiency, costs), there is a desire to converge these separate networks into one physical infrastructure, while still providing the isolation, security, and responsiveness needed by the organization.

High Level Converged Network Infrastructure Design

Our design of the converged network infrastructure for a health care organization is based on the hierarchical, three-layer model: core, distribution, and access layers. This hierarchy establishes the foundation and connectivity for the entire network, as shown below. It is a resilient network that is easy to understand and easy to troubleshoot.



Within each layer are redundant modules that serve a specific role in that layer. The hierarchy allows changes or upgrades to be performed at one layer in the hierarchy without disruption or significant changes to the other layers. End-do-end connectivity

Healthcare Industry Case Study

Practitioner
Forensics

Scenario

Post Covid-19, a local nursing home, Green Lantern Castle, is hosting a family visitation event. This is a major event in which families of patients, and patients who are able, are attending a cookout on the property.

Two of the families are previous acquaintances. During the event and ensuing conversations, the members of these two families, raised concern that their family member is either (sometimes) not responding to pain medication, or worse, not always receiving pain medication.

These two families decided to perform their own informal investigation. They scheduled specific times of day to visit their loved ones, making note of their pain levels. During this investigation, spanning a two-week period, they noticed a trend. During the times they felt their loved ones were in greater pain, a particular caregiver was always on duty.

These families share their suspicions with the CEO of Green Lantern. As a result, the CEO has requested that IT perform a digital forensics examination of all computer systems involved in the medication dispensary.

Dispensing Medications:

The medication dispensary uses an audit trail to prevent mishandling of pharmaceuticals. The system is set up with multiple checks and balances.

1. Caregiver enters their individual access code
2. Caregiver with search for patient name
3. Patient's medication list will appear on the screen
4. Caregiver selects the medication for the list
5. The storage bin housing the medication is provided on the screen
6. Caregiver maneuvers to the correct bin
7. If medication is a Schedule II narcotic, caregiver is required to enter his/her individual access code again
8. Upon administering medications, caregiver is required to scan the patient's barcode provided just inside the door of the patient's room

Healthcare Industry Context

Task 1

Your role is a forensic examiner with IT from Green Lantern Castle facility

Download the forensic image of the computer system containing all medication and patient logs. Perform a forensic examination of the computer. Document all steps performed in the examination. Provide a description of all evidence that may point to a problem with dispensing of medication of pain medications. As the examiner, create your own forensic report, and create a report containing the evidence from the Autopsy forensics software.

Practitioner Blockchain

Knowledge Check

How could a blockchain network between payers (insurers), healthcare systems, and patient owned data, help overcome barriers for prior authorizations and billing claims? (check all that apply)

- [ ] Less missing information
- [ ] Proper formatting
- [ ] Correct patient name/ identification
- [ ] Provide entire medical record

SUBMIT

- For most of the modules, the healthcare industry focus is readily separable so can easily replace with different industries
  - This module has deeper integration to highlight blockchain's applicability to healthcare

Practitioner
Blockchain

Homework #4: Blockchain and Healthcare Use Cases: *IBM Health Passport is an example of a healthcare use case which leverages the features of blockchain to solve a healthcare challenge.* https://www.ibm.com/products/digital-health-pass (2 hours)

	IBM Health Passport Blockchain Use Case
Problem(s) that a blockchain network could solve	After the onset of the covid019 pandemic, a new problem that society has not faced for a long time emerged: how to conduct "life as usual". Need: After restrictions on gathering are eased, how do we prove that we are well enough to gather and interact as we did before? -take people's word for it? -paper card certificates of vaccination? (paper cards get lost, can be counterfeit and do we really need to know where the vaccine is from, batch, etc.) -negative /positive testing status (or do we need to know where the test comes from, what batch and such) -delays and costs (people power), in transmitting validated information -data blocking -one system may not "talk" to the next
Application of BC Features	
Trust	Smart contracts allow participants into the blockchain: no counterfeit vaccine information can partake in the blockchain record for example.
Verification	Business rules set by the verifier (such as the stake holders designing the blockchain, for instance the state of NY so people can enter restaurants, concerts etc.) but the consent to share that verification is held by the user. Validated by "miners" to create a block or group of transactions that have been verified.
Data Provenance	Immutable data history allows the potential to provide data history from data origin regardless of episodes and incidents vs. fragmented or episodic information. The innate design of blockchain technology is based on a genesis node and subsequent nodes tied together directionally by hashes, creating a one way directional ledger.
HIPAA (patient right to privacy of HI)	The blockchain can allow necessary information to be connected to create a affirmative or negative result (green light or red light scenario) without divulging details such as type of vaccine, where received, patient age and other private health information). Patient controls what data is shared and level of privacy. Not having to request from a health system or provider adds another level of privacy.
Industry Adoption Standards	All stake holders communicating on the blockchain need to have the same API (Application Programming Interface) standards, a known challenge in health care because of variable electronic health record APIs. Most health records do not allow for efficient flow of information from one to another because of the privacy and proprietary nature of

- For most of the modules, the healthcare industry focus is readily separable so can easily replace with different industries
  - This module has deeper integration to highlight blockchain's applicability to healthcare

Practitioner
Blockchain

Homework: Part One Who Should Control the Data? and Evolving Governance

View conversation with Judah Thornewill, PhD, about the state and future of personally owned, person-centered, interoperable health records. (35 minutes)

- For most of the modules, the healthcare industry focus is readily separable so can easily replace with different industries
  - This module has deeper integration to highlight blockchain's applicability to healthcare

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

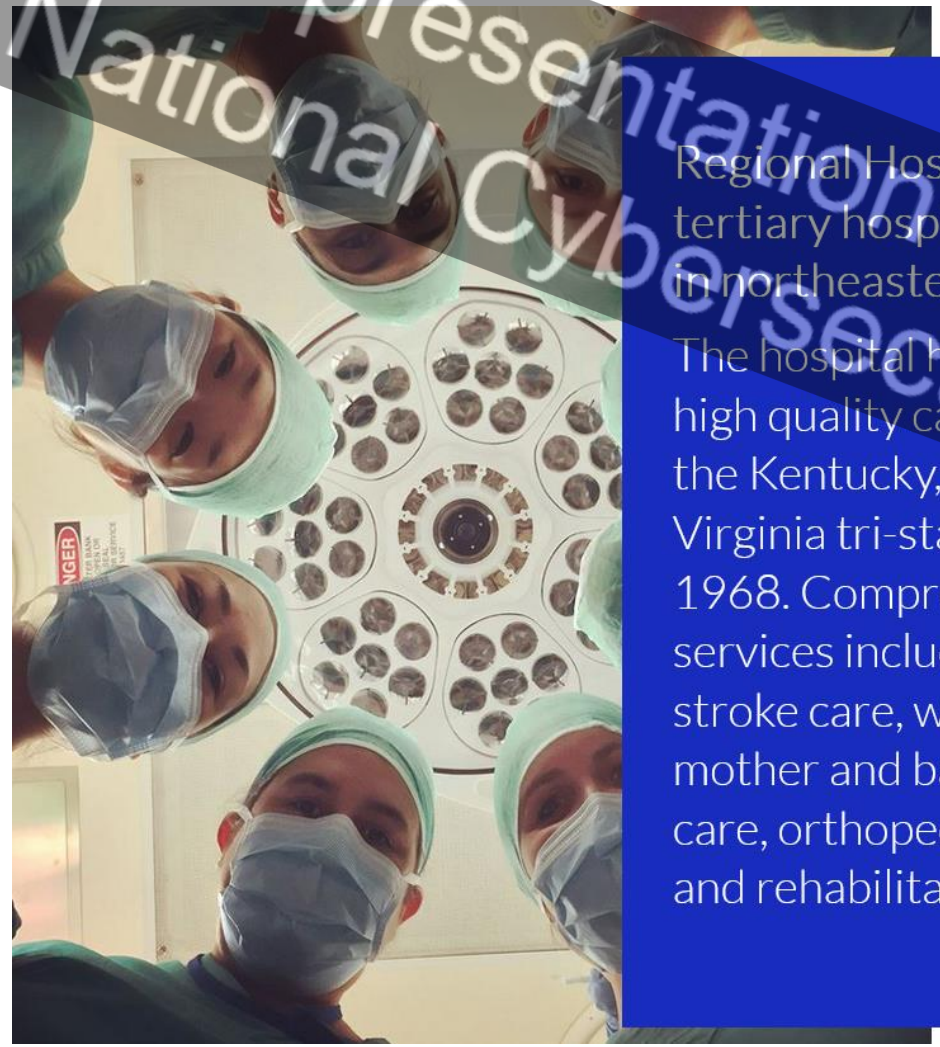
Professional

(Badges = Azure IoT, RPA and Power Automate & Threat Modeling)

- **DB Security**
- **Cloud Security**
- **IoT**
- **Post Quantum Cryptography**
- **Risk Analysis**
- **Robotic Process Automation Analysis**
- **Healthcare Capstone**

- The Professional level builds on the Explorer and Practitioner experience
- Culminates in Capstone module designed fully within healthcare industry context
  - Requires students apply knowledge and skills developed in earlier modules
  - Strong focus on critical thinking
  - Direct use of NIST CSF

Professional
Healthcare Capstone



Regional Hospital is a 500-bed tertiary hospital facility located in northeastern Kentucky.

The hospital has been providing high quality care for patients in the Kentucky, Ohio, and West Virginia tri-state area since 1968. Comprehensive patient services include heart and stroke care, women's health, mother and baby care, cancer care, orthopedics, neurology, and rehabilitation services.

Capstone: Introduction

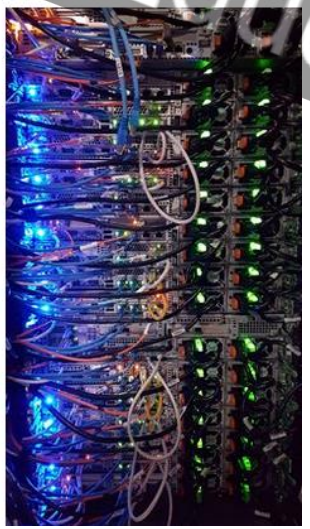
Professional
Healthcare Capstone

1
2
3
4
5
6

Hour 0

It's the Friday afternoon before a three-day weekend.

A network intrusion alert warns of increased network activity related to the electronic medical records (EMR) system as well as other servers and devices on the network.



Capstone: Hour 0

Professional
Healthcare Capstone

1. Many systems are down across the network.
2.
3.
4. Employees are reporting that they are unable to access the electronic medical records system.
5.
6. Patients are contacting the IT Helpdesk with complaints that the patient portal is not accessible.

Capstone: Hour 0

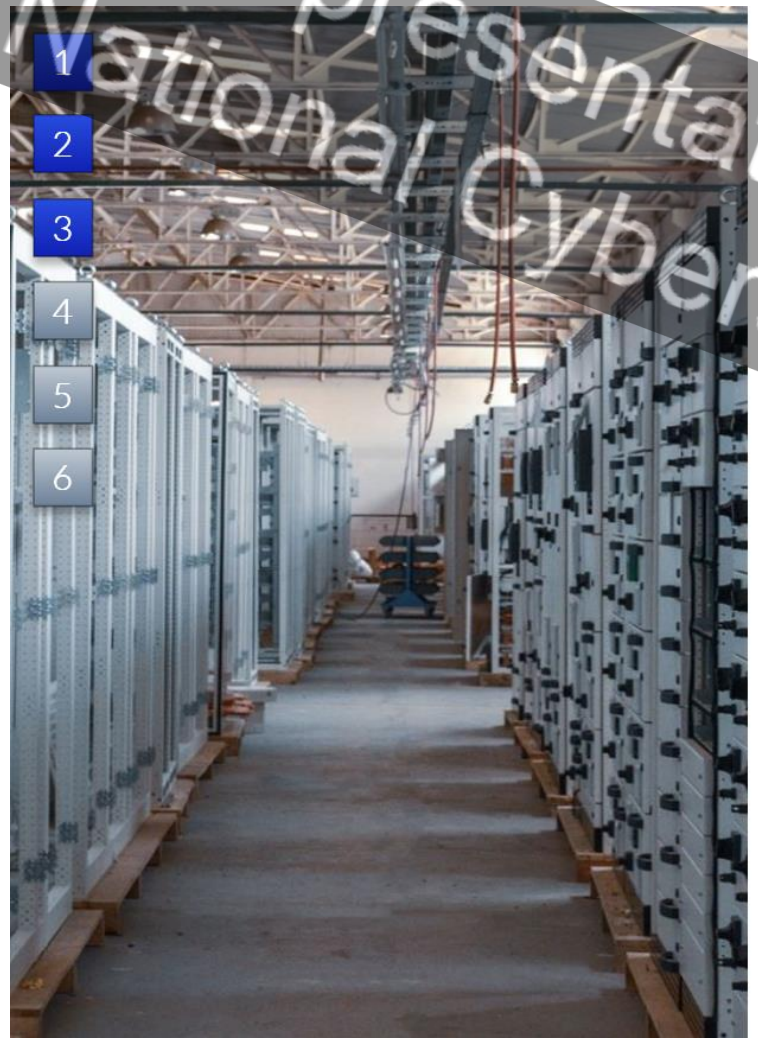
Professional
Healthcare Capstone

The IT department believes that a Ryuk ransomware attack involving electronic medical records is underway and has notified all offices and facilities to switch to downtime procedures immediately.

Please read this article on Ryuk.

Capstone: Hour 0

Professional
Healthcare Capstone



Hour 32

The initial forensics analysis indicates that offsite backups of Regional Hospital systems are intact, but local backups have been encrypted by the ransomware and so cannot be used to restore systems.

Capstone: Hour 32

Professional
Healthcare Capstone

Capstone: Hour 32

Professional
Healthcare Capstone

After you have reviewed section 3, take some time to answer the attached questions. Download the document and type your answers to each question. Once you have typed up your answers upload the document to complete the assignment.

[Answer length: 3-4 paragraphs]

1. Should the organization just pay the ransom? Explain, addressing:
    a. Is this legal?
    b. Is this ethical? If your answers to these questions differ, explain.
    c. Who do you think should be involved in approval (or disapproval) of such payment?
    d. What if the attacker doesn't provide the decryption key/protocol after payment?

See: Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments – from Treasury Department

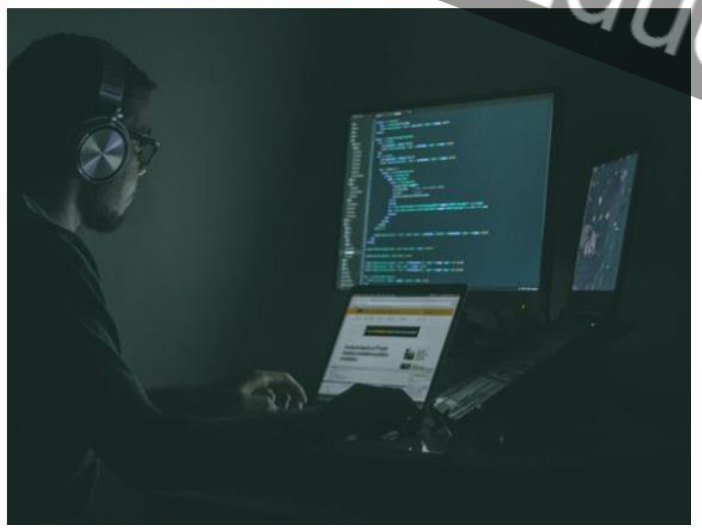
Capstone: Hour 32

Professional
Healthcare Capstone

1
2
3
4
5
6

Hour 52

The leadership team of **Regional Hospital** has authorized a restoration attempt of systems from the last offline backup. Recall, the last backup successfully transferred offsite is from 6 hours before the ransomware attack was initiated (at Hour 0).



Capstone: Hour 52

Professional
Healthcare Capstone

1
2
3
4
5
6

Hour 64

The following forensics report has been provided by experts on the attack (Click on the link to download the report):

Forensic Report

Capstone: Hour 64

Professional
Healthcare Capstone

1.
2.
3.
4.
5.
6.

The bad news is the forensic analysis has confirmed the ransomware was a variant with **data exfiltration capabilities**, which potentially accessed your entire patient data base, including medical information and Social Security numbers.

Capstone: Hour 64

Professional
Healthcare Capstone

After you have reviewed section 5, take some time to answer the attached questions. Download the document and type your answers to each question. Once you have typed up your answers upload the document to complete the assignment.

[Answer length: 2 paragraphs]

1. Who must be notified and when? [The patient or their personal representative, HHS, consumer reporting agencies, the media, etc.? State data breach requirements can require more but not less than the Federal requirements.] Hint: You get these numbers from the forensics report.

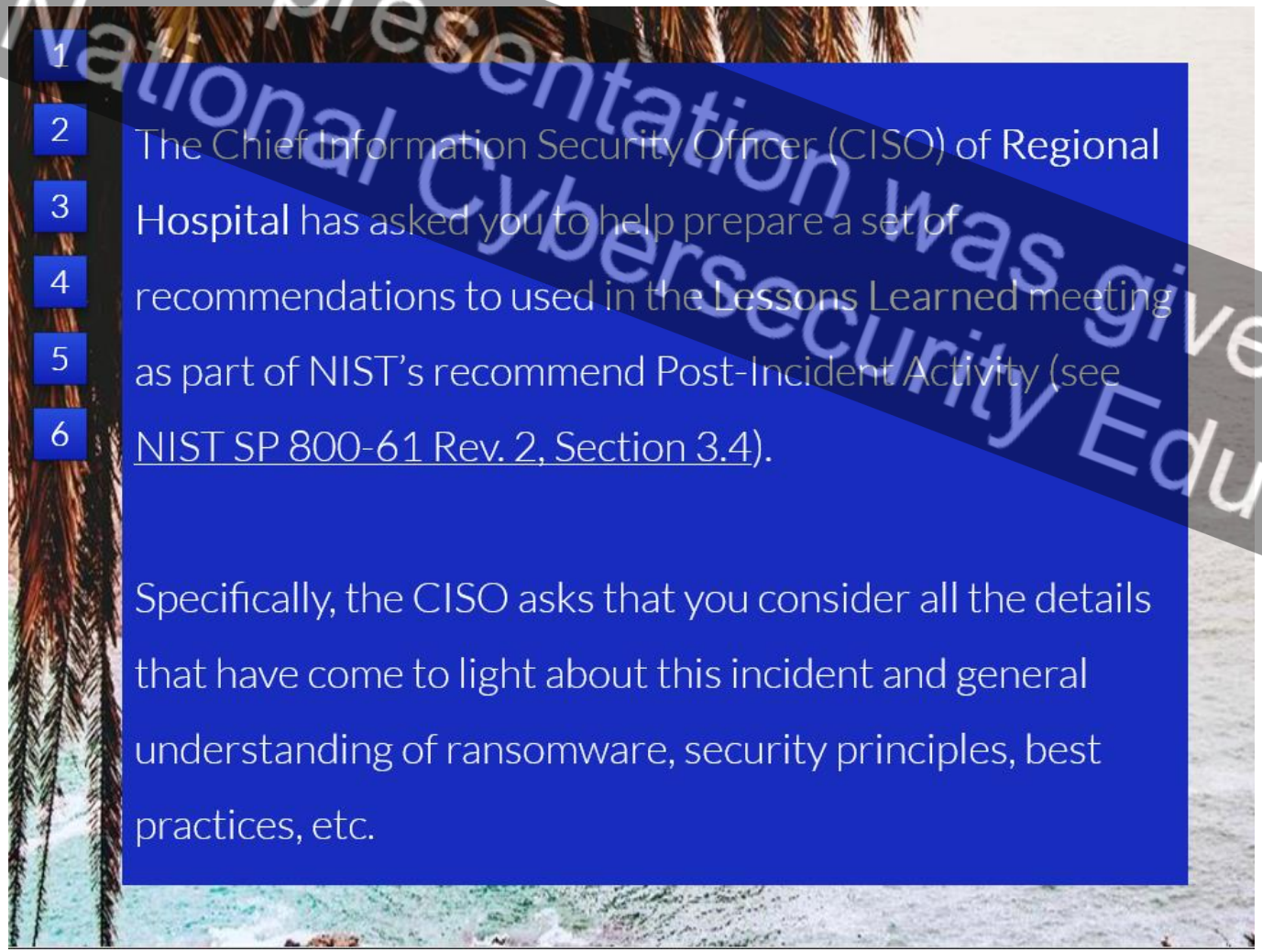
    a. Note: Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Covered Entity or Business Associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment. Unfortunately, "compromise" is not well defined.

    b. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

    c. For more information on breach notifications: https://www.bakerlaw.com/BreachNotificationLawMap

Capstone: Hour 64

Professional
Healthcare Capstone



Capstone: Conclusion

Professional
Healthcare Capstone

After you have reviewed section 6, take some time to answer the attached questions. Download the document and type your answers to each question. Once you have typed up your answers upload the document to complete the assignment.

[Answer length: at least 2 pages]

1. What are 5 recommendations (in priority order) that you would suggest the organization take to avoid/mitigate similar attacks and why?

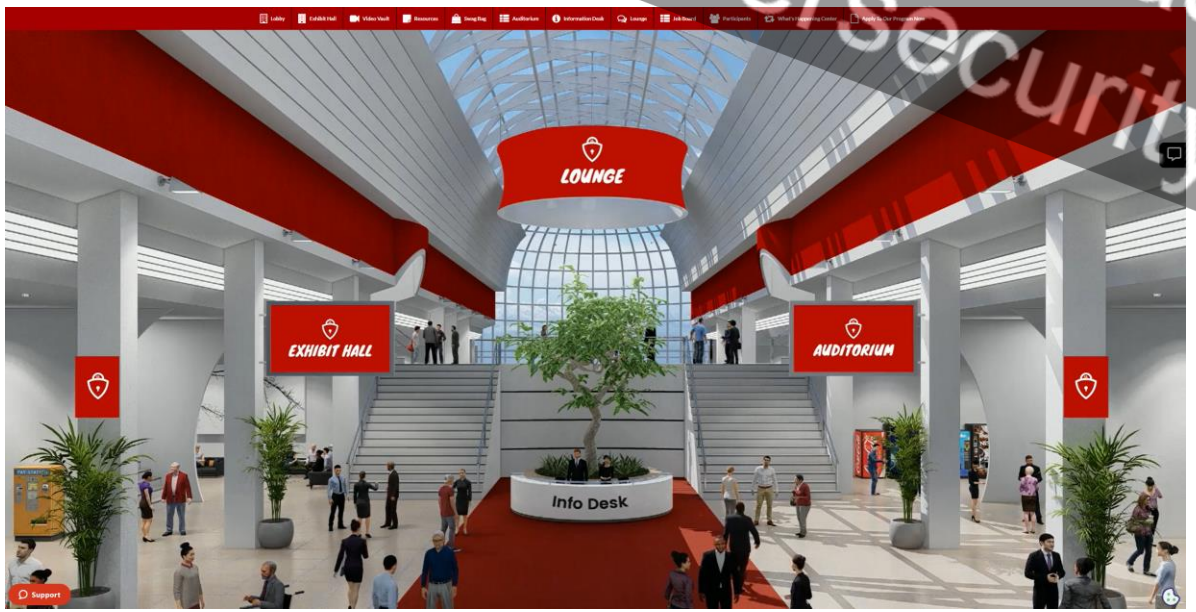
2. Which area(s) of the NIST Cybersecurity Framework (CSF) do you think needs to be reinforced and why?

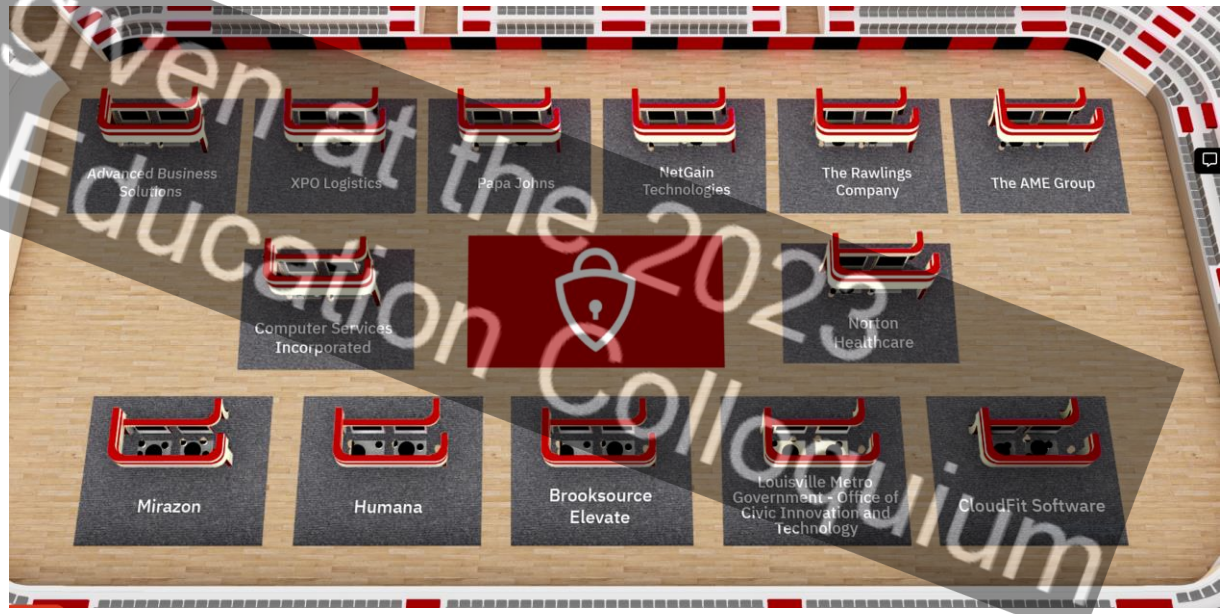
Capstone: Conclusion

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

Virtual Career Fairs





CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

Digital Badges & Degree Pathways

- Digital badges are awarded throughout the program from top technology vendors
- Upon completion of the entire program students, earn a **Cybersecurity Workforce Development certificate** (non-academic)
- With program milestones, students issued Coalition digital badges
  - These demonstrate that learners have achieved foundational cybersecurity knowledge, skills, and abilities
- Interested students continue their studies through our **Coalition Pathways to Success** that offer cybersecurity-related degrees from the Associate's level all the way up to a doctorate from our Coalition schools

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

- Gaming Component consists of:
  - Free mobile app available on Apple and Google
  - Competency based questions
  - Fun scoring/competition
- Virtual and Augmented Reality being developed now

- Created several smaller bundles of modules around related concepts
  - Offers a more focused and shorter time commit way to access the content
  - Some outreach with community orgs to create affinity cohorts

- Content is moving into Clark!

Our **Industry Advisory Board** has been critical to the success of our pilot program, but special thanks go to the following organizations for sharing so generously of their time and expertise:

Baptist Health
Humana
IBM
Knox Regional Development Alliance

The Healthcare Capstone Project, especially, benefited from the gracious participation of **Michael Erickson**, Chief Information Security Officer for Baptist Health.

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

Supported via NCAE-C-003-2020 Grant

THANK you!

Always looking to collaborate

Grateful for your attention

On behalf of the coalition:

Drs. Sharon Kerrick, Adel Elmaghraby, Andrew Wright

University of Louisville

sharon.kerrick@louisville.edu, adel.elmaghraby@louisville.edu, andrew.wright@louisville.edu