# Cybersecurity Fundamentals (6302)
# Teacher Resources

## Instructional Scenarios

### Risk/Vulnerabilities/Management, Oh My!

**Duty/Concept Area(s):** Exploring Cybersecurity Fundamentals

**Scenario:**

> You have been hired by the Trigon Corporation to create a series of presentations on security risks. The president wants his employees to be knowledgeable of the types of cybersecurity threats to the company and its employees.

**Big Question:**

> What are risk and vulnerabilities, and how does a company manage them?

**Focused Questions:**

1. What is the definition of *risk*?
2. What is the definition of *vulnerability*?
3. Why do organizations need to manage risk?
4. Why are the basic concepts of cybersecurity risk management?

**Project-Based Assessment:**

Read the following paper: An Introduction to Information System Risk Management

Create a Power Point to present to the users of Trigon. The Power Point should include an appropriate background, pictures, and the following information on the slides:

- Introduction
- Definition of *risk* and an example.
- Definition of *vulnerability* and two examples.
- Explanation of why users need to manage risk.
- Explanation of the concepts of managing risk. A slide should be done for each of these concepts and examples of where each might be used should be provided (these are the same as in economics and personal finance):
    - Risk Mitigation
    - Risk Transfer
    - Risk Avoidance

- Risk Acceptance

**Resources:**

- **VA Cyber Range**
- Cybersecurity Risks

## Threats and Threat Actors – Not Just External Any More

**Duty/Concept Area(s):** Describe cybersecurity threats to an organization.

**Scenario:**

You have been hired by a large bank in Virginia. They have asked you to detail what threats they might expect to their network and business. Specifically, they would like to know *who* might attack their network and *how* the attack would occur.

**Big Question:**

Can you describe the cybersecurity threats to an organization?

**Focused Questions:**

1. Who are the threat actors?
2. What are the attack types?
3. What types of malware are out there?

**Project-Based Assessment:**

Watch the following videos (Professor Messer):

- Professor Messer's SY0-501CompTIA Security+ Course
- Section 1.1 – Malware (all)
- Section 1.2 – Attack Types (all)
- Section 1.3 – Threat Actors

A bank with a large footprint in the Commonwealth of Virginia is potentially at risk for cyber threats.

You have been asked to write a report that details the following:

- Who are the top two threat actors?
  - Why are they the most concerning?
  - What can they affect within the network?
- What are the top five attacks the bank faces regarding its internal network?
  - How do they work?
  - Why are they the top ones?
  - How would they affect the business/network?
- What are the top two attacks to the bank's web-facing systems?
  - How do they work?
  - What makes these attacks the most prevalent?
  - How would they affect the business/network?

For this report, follow APA format and cite a minimum of five other references.

**Resources:**

- World's Biggest Data Breaches & Hacks, Information is Beautiful

- Cyber.Org, Instructure
- Open Web Application Security Project (OWASP) Top Ten, OWASP Foundation

## We Have Standards?

**Duty/Concept Area(s):** Discuss national or industry standards/regulations that relate to cybersecurity.

**Scenario:**

You would like to leave your position at the hospital to enter the field of education or pursue a position at the Department of Defense. How do you research the differences in regulations regarding cybersecurity in this field?

**Big Question:**

What are the industry standards/regulations that relate to cybersecurity?

**Focused Questions:**

1 What is PCI DSS?
2 What is FERPA?
3 What is HIPPA?
4 What is GDPR?
5 What is NIST?
6 What is ISO?

**Project-Based Assessment:**

Arrange students into groups of two or three, or make this an individual assignment. Research regulations and frameworks for security. Choose a total of ten different frameworks and provide the following information for each in chart format:

- What types of business are these targeting/required for?
- What are the overall basic requirements?
- What and who is it designed to protect?
- What are the penalties for not following the specific regulation?

**Resources:**

- Infosecurity Magazine, Infosecurity Group
- 23 Top Cybersecurity Frameworks, CyberExperts
- Cybersecurity Frameworks 101 – The Complete Guide, Prey Project

## Cybersecurity – Where Can They Get Me?

**Duty/Concept Area(s):** Describe the cyberattack surface of various organizations.

**Scenario:**

You have been hired by a contractor from the Department of Defense to review their risk factors and make suggestions on how to decrease their attack surface. They have

- communications (wired/wireless)
- connections to the Internet for employees to use
- facilities within five miles of each other
- door locks as the only form of physical security into the building
- credit card payments accepted over the web.

**Big Question:**

Can you describe what cybersecurity is and what it is exactly that businesses want to protect?

**Focused Questions:**

1 What is important for companies to protect?
2 What are the differences in the definition of cybersecurity?
3 Why is cybersecurity important?

**Project-Based Assessment:**

Research how to reduce your attack surface, then review the scenario. Determine what attack areas are wide open, which ones you would fix, and how. Share these with your fellow students in a discussion.

**Resources:**

- CyberOrg Cyber Business Module: How Businesses Secure Information

## Cybersecurity: How to Help to Avoid a "Gotcha"?

**Duty/Concept Area(s):** Analyze risks affecting critical infrastructure.

**Scenario:**

You have been hired by a company to make a presentation to the Department of Homeland Security about a specific piece of critical infrastructure.

**Big Question:**

What are the critical infrastructure areas found in cybersecurity? How can they be threatened, and how can they be protected?

**Focused Questions:**

1. What threatens our critical infrastructure?
2. What are the 16 critical infrastructure areas?
3. How are threats evolving?
4. How do those threats relate to these infrastructure areas?

**Project-Based Assessment:**

Arrange students into research groups of two or three to gather required information for the presentation.

Starting point: Critical Infrastructure Sectors.

- Research the selected sector.
- Create three attack scenarios that focus on ways the sector can be taken down:
  - Cyberattacks (required)
  - Terrorism
  - Pandemics
  - Weather
  - Technical failures
- Create a game plan and document the potential plans of attack.
- Create at least three methods of preventing those types of attacks.
- Present those methods as a classroom example of a presentation to the Department of Homeland Security.

| Sector-Specific Agency | Critical Infrastructure and Key Resources Sector |
|---|---|
| Department of Agriculture[a]<br>Department of Health and Human Services[b] | Agriculture and Food |
| Department of Defense[c] | Defense Industrial Base |
| Department of Energy | Energy[d] |
| Department of Health and Human Services | Healthcare and Public Health |
| Department of the Interior | National Monuments and Icons |
| Department of the Treasury | Banking and Finance |
| Environmental Protection Agency | Water[e] |
| Department of Homeland Security<br>*Office of Infrastructure Protection* | Chemical<br>Commercial Facilities<br>Critical Manufacturing<br>Dams<br>Emergency Services<br>Nuclear Reactors, Materials, and Waste |
| *Office of Cybersecurity and Communications* | Information Technology<br>Communications |
| *Transportation Security Administration* | Postal and Shipping |
| *Transportation Security Administration*<br>*United States Coast Guard*[f] | Transportation Systems[g] |
| *Immigration and Customs Enforcement, Federal Protective Service* | Government Facilities[h] |

| Sector-Specific Agency | Critical Infrastructure and Key Resources Sector |
|---|---|
| Department of Agriculture[a]<br>Department of Health and Human Services[b] | Agriculture and Food |
| Department of Defense[c] | Defense Industrial Base |
| Department of Energy | Energy[d] |
| Department of Health and Human Services | Healthcare and Public Health |
| Department of the Interior | National Monuments and Icons |
| Department of the Treasury | Banking and Finance |
| Environmental Protection Agency | Water[e] |
| Department of Homeland Security<br>*Office of Infrastructure Protection* | Chemical<br>Commercial Facilities<br>Critical Manufacturing<br>Dams<br>Emergency Services<br>Nuclear Reactors, Materials, and Waste |
| *Office of Cybersecurity and Communications* | Information Technology<br>Communications |
| *Transportation Security Administration* | Postal and Shipping |
| *Transportation Security Administration*<br>*United States Coast Guard*[f] | Transportation Systems[g] |
| *Immigration and Customs Enforcement, Federal Protective Service* | Government Facilities[h] |

Source: National Infrastructure Protection Plan, Department of Homeland Security

**Resources:**

- Cybersecurity and Infrastructure Security Agency
- Critical Infrastructure Security, Department of Homeland Security
- CYBER.ORG, Cyber Innovation Center 2020
- 2017 Infrastructure Report Card, American Society of Civil Engineers

## Can You Secure a Home From a Cyberattack?

**Duty/Concept Area(s):** Understanding Cyber Threats and Vulnerabilities

**Scenario:**

You and your partners are developing a *Blue Team* defense system for a personal residence home. After reviewing the home plan, the team realizes that there are physical and digital weaknesses that need to be secured to protect the property, personal items, important documents, and digital access.

The home owners requested that the following be addressed and implemented:

- How is unauthorized access gained to the home and the home network?
- How will the home office be secured?
- Will the homeowners have access to necessary protections if they are on a budget?
- Can their home and data be protected in a way that prevents anyone from being harmed?

**Big Question:**

How can businesses, residences, and users protect themselves from both physical & cyber threats?

**Focused Questions:**

1. Why do we need to protect our system?
2. How can someone gain unauthorized access to a physical location and network?
3. Can you predict and prevent all attacks?
4. Can you make anything 100 percent secure?

**Project-Based Assessment:**

Complete a small group activity threat modeling a home, taking on the mindset of *Blue Team* to protect the home. When the activity is completed, have the groups switch plans and take on the mindset of the *Red Team* to determine if there are any vulnerabilities in the plans. Use the link in the resources to access the lessons.

**Resources:**

- The Security Mindset: Cybersecurity through Threat Modeling
- Open Source Security, pfSense, Electric Sheep Fencing, LLC

## Who's Data Is It, Anyway?

**Duty/Concept Area(s):** Exploring Ethics as it Relates to Cybersecurity

**Scenario:**

One responsibility of the department store's security team is to monitor free Wi-Fi traffic to make sure no one is conducting illegal activity over the store's wireless network. In the course of normal monitoring activities, the security team intercepts emails between two people who are experiencing serious financial problems. The contents of these emails are in plain text and can be easily viewed by common packet sniffing tools.

Both people have recently been laid off from their jobs. The emails include details such as the couple's car recently being repossessed and a pending foreclosure on their house. While it seems unlikely that the couple will be able to pay off any future credit card bills, the couple's store credit account is still current and in good standing. The couple gathers a rather large and expensive selection of products, and they tell the store clerk to charge the items to their store credit account. The store's management, however, has already closed out the couple's account based on the intercepted emails.

**Big Question:**

Can the store ethically intercept private conversations taking place across a network connection that they own and provide to customers free of charge?

**Focused Questions:**

1. What expectation of privacy does the couple have in this situation?
2. What could the couple do to protect themselves from such unwanted scrutiny?
3. How does the store balance its obligation to prevent illegal activity across its network with a customer's right to privacy?

**Project-Based Assessment:**

Class discussion/role play illustrating obligations and rights of both the customer and the store.

## What's the Big Deal About Data Privacy?

**Duty/Concept Area(s):** Exploring Data Privacy

**Scenario:**

You have been hired to review a client's online privacy. They have been hacked, and you are looking at their potential profile and posting issues to help them have a more secure online experience. The client is also asking how their information can be exploited and used by other people and companies.

**Big Question:**

How can users protect themselves and their data from being exploited?

**Focused Questions:**

1. What are the risks associated with posting personal information?
2. How do you protect your privacy on social media and commercial websites?
3. What kind of information is being collected on the sites, platforms, and browsers that you use?
4. What are the benefits and risks of online tracking for users?
5. How do you protect yourself from online tracking?

**Project-Based Assessment:**

- In a small group, review a fictional public social media network profile. Prepare a presentation
  - reporting potential privacy issues
  - offering suggestions on how to protect from online tracking from other people and companies
  - offering solutions to ensure private information is secure.
- Use the first link under Resources to access the lesson and examples of profiles for this assessment. You may also create multiple profiles for each group to research and present.

Links have been provided below to use as projects, activities, and assessments.

**Resources:**

- The Invisible Machine: Big Data and You, The eQuality Project, Media Smarts
- 23 Great Lesson Plans for Internet Safety, Common Sense Media
- The Big Data Dilemma, Common Sense Media
- Debating the Privacy Line, Common Sense Media
- Privacy and Internet Life: Lesson Plan for Intermediate Classrooms, Common Sense Media
- Privacy Badger, Electronic Frontier Foundation

## Big Data, Little Data

**Duty/Concept Area(s):** Examining Data Security as it Relates to Cybersecurity

**Scenario:**

You decide you want to purchase a Bluetooth speaker. You visit Amazon.com first. When you enter "Bluetooth Speaker" into the search bar, you receive a lot of results. You also find you can filter your criteria by

- price
- speed of shipment
- type of phones compatibility
- special features
- manufacturer
- a number of other criteria.

When you create a Google search for "Bluetooth Speaker" the results are very different, and you can't really filter them in the same ways. Why is this?

**Big Question:**

In what ways are companies able to tailor data to your specifications and interests?

**Focused Questions:**

1. Where is this data being stored? Is it a type of software?
2. How can the specified criteria be filtered so quickly?
3. Why do different kinds of searches vary so much?
4. Are there different ways of accessing all of this data?

**Project-Based Assessment:**

Create a simple relational database and design a query that will filter the data based on user selections. It should

- Demonstrate ways in which the data could be "tainted" to cause it to not function properly.
- Examine ways to make queries less exact (i.e. like or wildcard queries)
- Look at the difference between a natural language query and a SQL query.

**Resources:**

- What are relational databases?
- Access 2019: How to Create an Access Database

## Do I Really Need to Give Access to That?

**Duty/Concept Area(s):** 84 – 93/Securing Operating Systems

**Scenario:**

John plugs his smartphone into his school laptop. A message box appears asking, "Do you want to download your photos onto this device?" What should he do?

**Big Question:**

Why is it important to know about security parameters like the different types of access controls (e.g. rights and permissions)?

**Focused Questions:**

- Different operating systems allow users to automatically upload files from one device to another. Why should this be important to you?
- Looking at this scenario, what would happen if John clicks "Allow"?
- Would John still have privacy rights to his photos if they are uploaded onto his school computer?
- Can anyone who has access to his laptop now see those photos?
- What can you do to keep your information private?

**Resources:**

Show App permissions - What you need to know and discuss why companies harvest your data.

## Internet of Things - How does Alexa really work?

**Duty/Concept Area(s):** Exploring Cybersecurity Implications for Current and Emerging Technologies

**Scenario:**

Susie has an Amazon Alexa device in her home, and she uses it to play her favorite music and call her friends. Amazon Alexa is an example of an Internet of Things (IoT). What are the pros and cons of this type of IoT?

**Big Question:**

What are the pros and cons of the Amazon Alexa IoT?

**Focused Questions:**

1. Is an IoT like Amazon Alexa always listening to you? If so, is that data stored? How is it used?
2. Can Amazon Alexa be hacked? How? Why would someone want to hack your Amazon Alexa?
3. How do you know if someone is dropping in on Amazon Alexa?

**Project-Based Assessment:**

- Have your students research the focus questions and share the information with the rest of the class. This can be a project or a quick 15-minute exercise.

**Resources:**

- Google
- Amazon Echo Privacy - Is your information safe?
- Optional project - Create your own IoT - full lesson plan

# Cyber Security and Cyber Forensics Infusion Units

Cyber Security and Cyber Forensic Infusion Units (CYBR) were designed to be infused with designated CTE courses to help students in those programs achieve additional, focused, validated tasks/competencies in personal and professional cyber security skills. These units are not mandatory, and, as such, the tasks/competencies are marked as "optional," to be taught at the instructor's discretion.

# Customer Service Infusion Units

Customer Service Infusion Units (CSIU) were designed to be infused with designated CTE courses to help students in those programs achieve additional, focused, validated tasks/competencies in customer service. These units are not mandatory, and, as such, the tasks/competencies are marked as "optional," to be taught at the instructor's discretion.

# Entrepreneurship Infusion Units

Entrepreneurship Infusion Units may be used to help students achieve additional, focused competencies and enhance the validated tasks/competencies related to identifying and starting a new business venture. Because the unit is a complement to certain designated courses and is not mandatory, all tasks/competencies are marked “optional.”