Shawn's C841 Keys to Success

1st - Read my introduction email
2nd - Read the Case Study and Task Requirements
3rd - **Read this document in full** & read entries in Course Announcements and Course Tips
4th - Complete the Tasks

- Use my task walkthrough videos, and task guidance spreadsheet to help with drafting your outline, papers and/or presentations [**single PPT per task option is my recommendation**]
- Once you have your draft, use the questions in the third column of the task guidance tab of the spreadsheet to cross check your work
- Check draft originality and similarity levels and adjust accordingly
- Submit your work and PASS!

Task Components

What to Produce

You must complete both tasks to complete the course. You must provide sufficient responses to the questions in each task using a file within the allowed file types section of your task requirements. You will submit only one file per task.

File Restrictions
*File name may contain only letters, numbers, spaces, and these symbols: ! - _ . * ' ( )*
File size limit: 200 MB
File types allowed: doc, docx, rtf, xls, xlsx, ppt, pptx, odt, pdf, txt, qt, mov, mpg, avi, mp3, wav, mp4, wma, flv, asf, mpeg, wmv, m4v, svg, tif, tiff, jpeg, jpg, gif, png, zip, rar, tar, 7z

I have shared PPT and WORD templates that you are more than welcome to use. Simply follow the instructions within them, flesh them out with your responses, run similarity checks and submit.

Page/Word Count Requirement Both Tasks

Page/Word Count Minimum

There is no specified minimum or maximum page or word count requirement for the tasks.

Originality Both Tasks

Originality and Similarity Standards

Your submission must be your original work. No more than a combined total of ***30%*** of the submission and no more than a ***10%*** match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly... ***Video on Reviewing Unicheck Reports-**

Sources Both Tasks

APA Formatting Requiremen

Q: Do I have to include in-text/in-line citations in my work?
A: No, you do not. However, **IF** you choose to quote, paraphrase, or summarize content from a source, **THEN** you must acknowledge that source using in-text/in-line citations and an accompanying reference page/reference slide. Your work can be 100% original work if you choose.
The one area from the entire assignment, where you may not be able to get around keeping your work fully original is Task #2 Part A1/A1a where you are asked to provide specific ethical guidelines used by other organizations. Since those guidelines will be those organizations' content, best practice to capture them would be for you to directly quote/paraphrase/summarize them.

Q: If I quote, paraphrase, or summarize content from a source, do I have to use APA format?
A: No, you do not. There is no specific writing style requirement for the assignment. This absence of a standard writing style however introduces ambiguity in what information is required for citations and reference lists that often leads to task returns for missing information. So, if you choose to quote, paraphrase, or summarize content from a source you should look to, at a minimum, include the core elements of **author, date,** and **title** for your citations and accompanying reference lists.
A safe bet is to just employ APA, or another style for the citation and references portion of your work regardless of how you format the whole work.

Q: If I want to quote, paraphrase, or summarize content from a source, where can I get help with formatting the citations and references?
A: There is no specified writing style you must use for the assignment, but there is a plethora of information on APA citations and references within the WGU Writing Center. https://my.wgu.edu/success-centers/writing-center/learning-resources Also, my favorite through most of my academic years was Purdue Owl Online Writing Lab, which has excellent guidance for citing and such for multiple writing styles to include APA and MLA. https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_formatting_and_style_guide/in_text_citations_the_basics.html

Q: I would like to quote, paraphrase, or summarize content from the course text to support one of my responses, where do I find the author and date information to acknowledge the text?
A: This information can be found on page 2 of the text. I have pasted it here for quick reference as well.
Grama, Joanna Lyn. (2015) Legal Issues in Information Security

Q: I would like to quote, paraphrase, or summarize content from the case study to support one of my responses, where do I find the author and date information to acknowledge the case study?
A: Use a no author, no date annotation for your citation i.e. (TechFite Case Study, n.d.) and a no date, no author with a "retrieved from" link for your reference page entry. i.e. TechFite Case Study, n.d. Retrieved from [copy/past task page URL where case study resides here]

Q: How much of my work can be quoted, paraphrased, or summarized content from a source?
A: *No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source.*
Q: Is properly cited information subject to the 30% total similarity threshold?
A: Yes. Your submission can have n*o more than a combined total of 30% similarity* ***even if cited correctly****.*

	Citation and Reference Example 1-No Specific Writing style
In-text	An ethical guideline used by the Information Systems Security Association (ISSA) states that members will "Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles" (ISSA Code of Ethics, n.d.).
Reference Page entry	Information Systems Security Association (ISSA) Code of Ethics. n.d. Retrieved from https://www.issa.org/issa-code-of-ethics/

	Citation and Reference Example 2-No Specific Writing style
In-text	According to Grama (2015), "the Internet is a protected computer because the Internet facilitates commerce between different states".
Reference Page Entry	Grama, J. (2015). *Legal issues in information security*, Second Edition. Burlington, MA

Task 1 Legal Analysis

CFAA

The Computer Fraud and Abuse Act (CFAA) covers the basic themes of *computer-related fraud activities*, and *protection from insiders that exceed their authority accessing records on protected computers*. Think about where an individual or group was involved in apparent or reasonably assumed fraud using a computer or who accessed information on a system they were not authorized to access. A protected computer is any of the following: A federal government computer; A financial institution computer; A computer used in interstate or foreign commerce. Under the statute, the Internet is a protected computer because the Internet facilitates commerce between different states. The CFAA definition of "financial institution" includes organizations that provide financial services to customers such as banking, investment, and insurance services.

The "computer affecting interstate commerce or communication" piece of the protected computer definition coupled with our current technological state in this day and time (we connect everything to the internet), significantly widens the aperture for qualifying devices as "protected" and thereby subjected to prosecution under CFAA.

The fact that Techfite connects its network to the Internet to conduct business makes the computers within its network fall into the protected computer category. Therefore, any instances you observe in the case study involving intentional access to any of those computers without authorization would constitute a violation of CFAA. A good case example to add context and understanding is US vs Trotter.

The CFAA addresses the following types of criminal activity:

- Unauthorized access of national security information
- Unauthorized access to a government computer
- Compromising the confidentiality of a protected computer
- Unauthorized access to a protected computer with an intent to defraud
- Unauthorized access to a protected computer that causes damage
- Intentional transmission of malware, viruses, or worms that damage a protected computer
- Unauthorized trafficking of passwords or other computer access information that allows people to access other computers without authorization and with the intent to defraud
- Extortion involving threats to damage a protected computer

ECPA

The Electronic Communications Privacy Act (ECPA) governs access to stored electronic communications. This includes access to the contents of the communication and the headers and other transmission information. The ECPA is an amendment to the original Wiretap Act. Consider the ECPA, remember the act deals with restriction of *unauthorized access to electronic communications*. Electronic communications can be any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electric or photo optical system. Additionally, consider that electronic communications, as it pertains to the case study includes those in transit (across the wire, airways etc.), as well as those stored on information systems (an email or other communications capture stored on a computer drive or server); lastly, unauthorized access to pertinent components of communications are included as well i.e. contents of the communication as well as the headers and other transmission information. For your response to the task look to identify an instance from the case study involving **unauthorized access, use, disclosure, or interception of electronic communications.**

SOX

The main goal of the Sarbanes-Oxley Act of 2002 (SOX) is to protect shareholders and investors from financial fraud. Think about how SOX applies to the company with respect to activities observed that may constitute violations of the act. i.e. was there any activity that occurred that would illegally exaggerate the company's appeal to persuade investors or to create a possible avenue for embezzlement? What is SOX's stance on auditing as compared to TechFIte's auditing policies, practices, or lack thereof? Keyword search "financial" within the case study and investigate finance-related activity the publicly traded company is engaged in.

Three Laws

Recommendation is to discuss how violations of the three laws already listed in the task requirements justify legal action. You do not have to use these laws, you may use any three that are applicable ts long as you accurately tie them to the activity in the case study and justify your response.

Duty of Due Care

Duty of due care refers to the effort made by an ordinarily prudent or reasonable party to avoid harm to another, taking the circumstances into account. It refers to the level of judgment, care, prudence, determination, and activity that a person would reasonably be expected to do under certain circumstances. A **duty of due care** is a person's obligation to avoid acts or omissions that can harm others. The level of duty that one person owes to another is based on the reasonable person standard. The reasonable person standard is a legal concept used to describe how an ordinary person would think and act.

Criminal Activity

Criminal procedure deals with the rules that courts follow in criminal law cases. It also includes the processes for investigating and punishing crimes. The federal and state governments have criminal codes. These codes specify the actions that constitute a *crime*. Crimes are wrongs against society. Crimes are prosecuted by the government against an alleged wrongdoer. The federal or state official with the power to pursue criminal cases is called a *prosecutor*.

Negligent Activity

Negligence torts are based on the premise that a person is liable for any injuries or harm that are the foreseeable consequences of his or her actions. In order to prove a negligence-based tort, a plaintiff must show that:

-The defendant owed the plaintiff a duty of due care
-The defendant breached his or her duty
-The breach of duty caused the plaintiff's foreseeable injuries
-The plaintiff was damaged

Actors and Victims

Based on the information and details that are provided, understanding of the law or concept associated with a given task question, you are develop feasible conclusions and articulate your reasoning for them in your answers. This applies for the questions you are asked to identify actors and victims in as well.

Let's say you have a case study states that Joe Robber was clearly captured on surveillance smashing through a window and committing a home burglary, making off with several items. This case study includes no other details, but you have questions for the task asking who the alleged culprit(s) and victim(s) of this crime were. Based on the information provided, you could feasibly state that:

-Joe Robber is the alleged criminal actor as evidenced in the case study by the video footage.

-The home owners are victims because their home was broken into and because they may have had belongings taken

-Any acquaintances of the home owners who had belongings taken from the home owners' home during the robbery are potentially victims as well.

Cybersecurity Policies

Information security policies will vary across organizations. This is because all organizations are different. They have different business goals. Their security needs aren't the same. Their cultures are different. The list of information security issues to address in a policy is endless. However, all organizations face some basic security issues. They should create policies to address these issues. You will select policies that will address the specific instances security needs on the company in the case study.

Task 2 Ethics and Cybersecurity Awareness

Ethical Guidelines and Standards

Few fields are free from ethical dilemmas and the need for professional guidance on how to do deal with such issues. Information technology is no exception; in fact, this field offers many more ethical challenges than one might think upon first consideration. Outlined below are some specific resources available to help guide IT professionals when they are faced with such ethical dilemmas. One avenue to identity ethical guidelines is to pull them from code of ethics documents.

- **Information Systems Security Association Code of Ethics**: https://www.issa.org/code-of-ethics/
- **ISC²**: https://www.isc2.org/Ethics
- **ASIS International**: https://www.asisonline.org/About-ASIS/Pages/Code-of-Ethics.aspx

View a listing of additional organizations to research ethical guidelines of for use in meeting your A1a requirement here https://cybersecurityventures.com/cybersecurity-associations/

SATE (Security | Awareness | Training | Education)

An important part of any information security program is the training and awareness component. This is because employees play a large role in meeting information security goals. Employee behavior can help protect data and IT resources. It also can be harmful. Employees who aren't aware of their responsibilities pose a threat. They may engage in risky online activities. These activities could harm the organization's IT resources. Their actions also could disclose data. They can subject an organization to liability. Training and awareness activities help reduce this threat.
Remember that intellectual property is the area of law that protects a person's creative ideas, inventions, and innovations. It's protected by patents, trade secrets, trademarks, and copyright.

Pay close attention to what constitutes “components” of a SATE program for this assignment in the task guidance spreadsheet.