# Case Study #2: Data Security & Data Loss Prevention

## Scenario

Congratulations on successfully completing your first briefing paper for Padgett-Beale! The management interns did so well that the Training Team has asked for your assistance in developing a second training module. The topic for this training module will be “Data Security and Data Loss Prevention for Travelers.”

This training topic was selected after two Padgett-Beale employees had sensitive corporate information and login credentials stolen from their mobile devices while they were traveling. One employee was traveling inside the United States. The other employee was out of the office for two weeks on a multi-country trip. In one case, it appears that the attackers gained access to both a company cellphone and a company-owned laptop. In the other, it appears that the active attack affected an employee’s personal laptop while she was using hotel provided Wi-Fi. This employee was using her personal laptop because her company laptop was in checked baggage (due to FAA and TSA restrictions) and was stolen while in the airline’s baggage handling system.

Fortunately, neither person had stored or accessed customer information from these devices. Both thefts were caught after attackers tried to exploit the stolen login credentials and could not get past the two-factor authentication requirement (security code generated an authenticator application on the employee’s corporate cell phone). During the *after action reviews* for these incidents, a training gap and a technology gap were identified. A policy gap, with respect to enforcing *least privilege* and *separation of duties* was also identified as a potential area of risk (too much access to sensitive data while traveling could exacerbate the risks of data loss).

 Your deliverable for this assignment will be a briefing paper that identifies and discusses five or more major issues that employees need to be aware of about this topic (Data Security and Data Loss Prevention for Travelers). After you identify and describe each security or privacy issue, include two to three additional points that employees should know. Try to keep a neutral tone, that is, you should focus on solutions not blame. You should also address the importance of protecting both personal and company owned devices and data while traveling. After you address the issues, identify and discuss at least 5 recommended solutions (include at least one technology solution and one policy solution). See the instructions below for additional information about length, formatting, and citing of sources.

## Research

1. Review the Week 1, 2, and 3 readings.
2. Read these articles about security tips for business travel (both US and foreign travel).
	1. <https://us.norton.com/internetsecurity-mobile-8-cyber-security-tips-for-business-travelers.html>
	2. <https://www.calyptix.com/top-threats/7-tips-data-security-business-travelers/>
	3. <http://www.redzonetech.net/blog/13-mobile-device-security-tips-foreign-business-travelers-china/>
	4. <http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Workplace-5-Key-Risks-and-a-Surprising-Challenge>
3. Research how a data loss prevention solution can help prevent data thefts. Begin with these resources:
	1. <https://www.symantec.com/connect/articles/how-symantec-data-loss-prevention-mobile-works-how-implement>
	2. <https://sierraware.com/blog/?p=212>
4. Research how two-factor authentication solutions can be used to prevent data thefts by attackers who have stolen a person’s login credentials. Begin with these resources:
	1. <https://docs.microsoft.com/en-us/azure/multi-factor-authentication/end-user/microsoft-authenticator-app-how-to>
	2. <https://www.google.com/landing/2step/>
	3. <https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access/securid-software-tokens>
5. Include in your discussion 3 or more additional technologies that could be implemented to help prevent data thefts originating from a business traveler’s mobile devices.
	1. Virtual Private Network
	2. Whole Disk Encryption
	3. Mobile Device Management (including remote wipe for stolen devices)

## Write

Write a 2 page briefing paper in which you present a summary of your research about the topic and your recommendations as to what should be included in the training module. Be choosy about what you include – the total training time available will be 30 minutes. Don’t be too choosy however. Your recommended content should be comprehensive and fully address the training topic.

At a minimum, your briefing paper for this case study must include the following:

1. An introduction to the case scenario and the topic (use the information above)
2. An analysis of the security and privacy issues that includes five or more key points about the topic (“data security and data loss prevention”). Remember to stay focused on business travelers and mobile devices (laptops, tablet computers, cell phones, etc.)
3. Recommendations for 5 or more *best practice* based actions that managers and employees should take to address the identified security and privacy issues. Include at least one recommendation for a technology based solution (e.g. VPN, Mobile Device Management, Whole Disk Encryption, etc.) Include at least one recommendation for a policy based solution, i.e. implementing access controls based upon least privilege and/or separation of duties.
4. A closing section in which you restate the key issues and your recommendations.

As you write your briefing paper, make sure that you address security issues using standard terms and definitions (<https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf>)

## Submit For Grading

Submit your research paper in MS Word format (.docx or .doc file) using the Case Study #1 Assignment in your assignment folder. (Attach your file to the assignment entry.)

## Additional Information

1. To save you time, a set of appropriate resources / reference materials has been included as part of this assignment. You must incorporate at least three of these resources into your final deliverable. You must also include one resource that you found on your own.
2. Your briefing paper should use standard terms and definitions for cybersecurity. See Course Content > Cybersecurity Concepts for recommended resources.
3. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be on a separate page at the end of your file. These pages do not count towards the assignment’s minimum page count. (An example and template file are available in the LEO classroom. See CSIA\_Basic\_Paper\_Template(APA\_6ed,Nov2014).docx file under Content > Course Resources.)
4. Your briefing paper should be professional in appearance with consistent use of fonts, font sizes, margins, etc. You should use headings to organize your paper. The CSIA program recommends that you follow standard APA formatting since this will give you a document that meets the “professional appearance” requirements. APA formatting guidelines and examples are found under Course Resources > APA Resources. An APA template file (MS Word format) has also been provided for your use CSIA\_Basic\_Paper\_Template(APA\_6ed,Nov2014).docx.
5. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.

You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.).