# MIS 5206
# Protection of Information Assets
## - Unit #2 -

## Case Study: Snowfall and a stolen laptop
## In-Class Exercise
## Section 401

# Case Study Teams
# Section 701

| Full Name | Email Address | Team |
|---|---|---|
| Lindsley, Jason A. | tug29037@temple.edu | 1 |
| Needle, Paul R. | tue82889@temple.edu | 1 |
| Yu, Xiaozhou | tuf12196@temple.edu | 1 |
| Eidenzon, Tal | tud12762@temple.edu | 1 |
| Thomas, Sheena L. | tue96537@temple.edu | 2 |
| Dabbas, Dima | tuf13663@temple.edu | 2 |
| Conard, Robert L. | tuk32920@temple.edu | 2 |
| Sun, Haixin | tuf74816@temple.edu | 2 |
| Pandya, Jaimin R. | tuc54538@temple.edu | 3 |
| Pitter, Tamekia | tuh31407@temple.edu | 3 |
| Shah, Sachin S. | tug87391@temple.edu | 3 |
| Ding, Shuyue | tug26714@temple.edu | 3 |
| Nguyen, Joseph | tug87199@temple.edu | 4 |
| Alkaysi, Ahmed A. | tub65791@temple.edu | 4 |
| Soroko, Arren D. | tue85820@temple.edu | 4 |
| Liu, Mengqiao | tug34745@temple.edu | 4 |
| Scheuren, James J. | tug06218@temple.edu | 5 |
| Rohrer, Frederic D. | tuf11403@temple.edu | 5 |
| Feldman, Joseph E. | tue56704@temple.edu | 5 |
| Lester, Iyana J. | tuc18754@temple.edu | 5 |
| Tartaglione, Eugene A. | tuf08694@temple.edu | 6 |
| Zimmerman, Matthew A. | tud09967@temple.edu | 6 |
| Gyamfi, Derrick A. | tuj39966@temple.edu | 6 |
| Yang, Xinye | tuf41830@temple.edu | 6 |
| Alahari, Sai Manogna L. | tuj21822@temple.edu | 7 |
| Parekh, Ami H. | tuf94220@temple.edu | 7 |
| Shah, Nauman T. | tue62043@temple.edu | 7 |
| Cheung, Heiang Y. | tub55844@temple.edu | 7 |
| Duani, Jonathan B. | tuc34780@temple.edu | 8 |
| Levinson, Ariana M. | tud04791@temple.edu | 8 |
| Jiles, Lezlie M. | ljiles@temple.edu | 8 |
| You, Zirui | tuf68884@temple.edu | 8 |

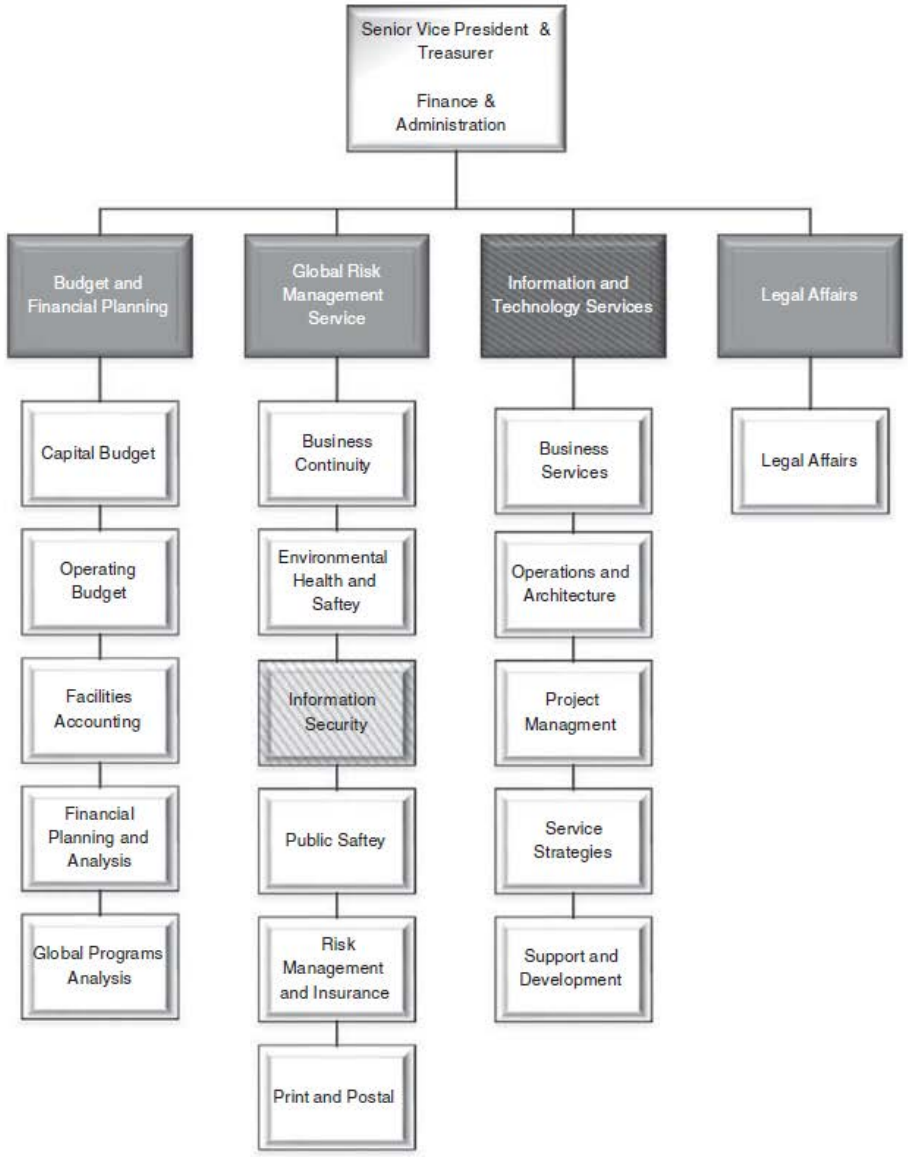
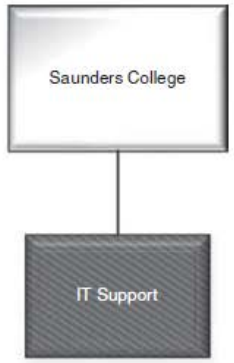



**Figure C1** Partial RIT administrative organization chart.




Case Study Analysis: "Snowfall and a stolen laptop"

1. Which organization does:
   - Dave Ballard report into?
     - Network Administrator
   - Nick Francesco report into?
     - Manager of Technical Services
   - Information Security Office (ISO) reside?

2. What information security reporting or organizational governance relationship exists between ISO and the organization(s) Ballard and Francesco report into?

# Recovering deleted data files

"On your computer, accessing "deleted" data can easily be done with one of many file undelete and data recovery programs widely available on the Internet. These programs are touted as conveniences, which in some cases, they are

- But when it comes to security, the way your computer deletes (or doesn't delete) your data is a liability
- Someone accessing your computer remotely (i.e. a hacker) could very easily "recover" your deleted data
- The same goes for someone who buys your used computer on eBay or digs your discarded, failed hard drive out of the dumpster

- This has been an issue for decades. Yet still, there are no built-in system operations designed for securely deleting your data. On the contrary, Windows tends to do everything it can to keep all historical data, in case you want to perform a system restore or recover a lost file."

https://www.r-studio.com/file-recovery-basics.html

*Francesco asked 'What student records did you have on your laptop?'*
*The Dean quickly replied 'None.'*

*Francesco clarified: "Until recently we used Social Security numbers to identify our students. Are you sure you didn't have any old class rosters, exams or other records on there?"*

*The Dean took a few seconds to deeply consider what he was asked. 'No. I am not teaching this semester, and **I deleted everything from previous semesters**.'*

# RIT Information Classifications

**A.** **Private** – a classification for information that is confidential which could be used for identity theft and has additional requirements associated with its protection. Private information includes:

A. Social Security Numbers (SSNs), Taxpayer Identification Number (TIN), or other national identification number
B. Driver's license numbers
C. Financial account information (bank account numbers (including checks), credit or debit card numbers, account numbers)

**B.** **Confidential** – a classification for information that is restricted on a need to know basis, that, because of legal, contractual, ethical, or other constraints, may not be accessed or communicated without specific authorization. Confidential information includes:

A. Educational records governed by the Family Educational Rights & Privacy Act (FERPA) that are not defined as directory information
B. University Identification Numbers (UIDs)
C. Employee and student health information as defined by Health Insurance Portability and Accountability Act (HIPAA)
D. Alumni and donor information
E. Employee personnel records
F. Employee personal information including: home address and telephone number; personal e-mail addresses, usernames, or passwords; and parent's surname before marriage
G. Management information, including communications or records of the Board of Trustees and senior administrators, designated as confidential
H. Faculty research or writing before publication or during the intellectual property protection process.
I. Third party information that RIT has agreed to hold confidential under a contract

**C.** **Internal** – a classification for information restricted to RIT faculty, staff, students, alumni, contractors, volunteers, and business associates for the conduct of University business. Examples include online building floor plans, specific library collections, etc.

**D.** **Public** – a classification for information that may be accessed or communicated by anyone without restriction.

*Francesco continued: 'Think about this carefully, because it has implications much bigger than you and me.* ***What proprietary Saunders data did you have on that laptop?'***

*The Dean replied, 'I really didn't have anything too important. It was committee notes, faculty salary information, stuff like that. It may have been confidential, but not really proprietary.'*

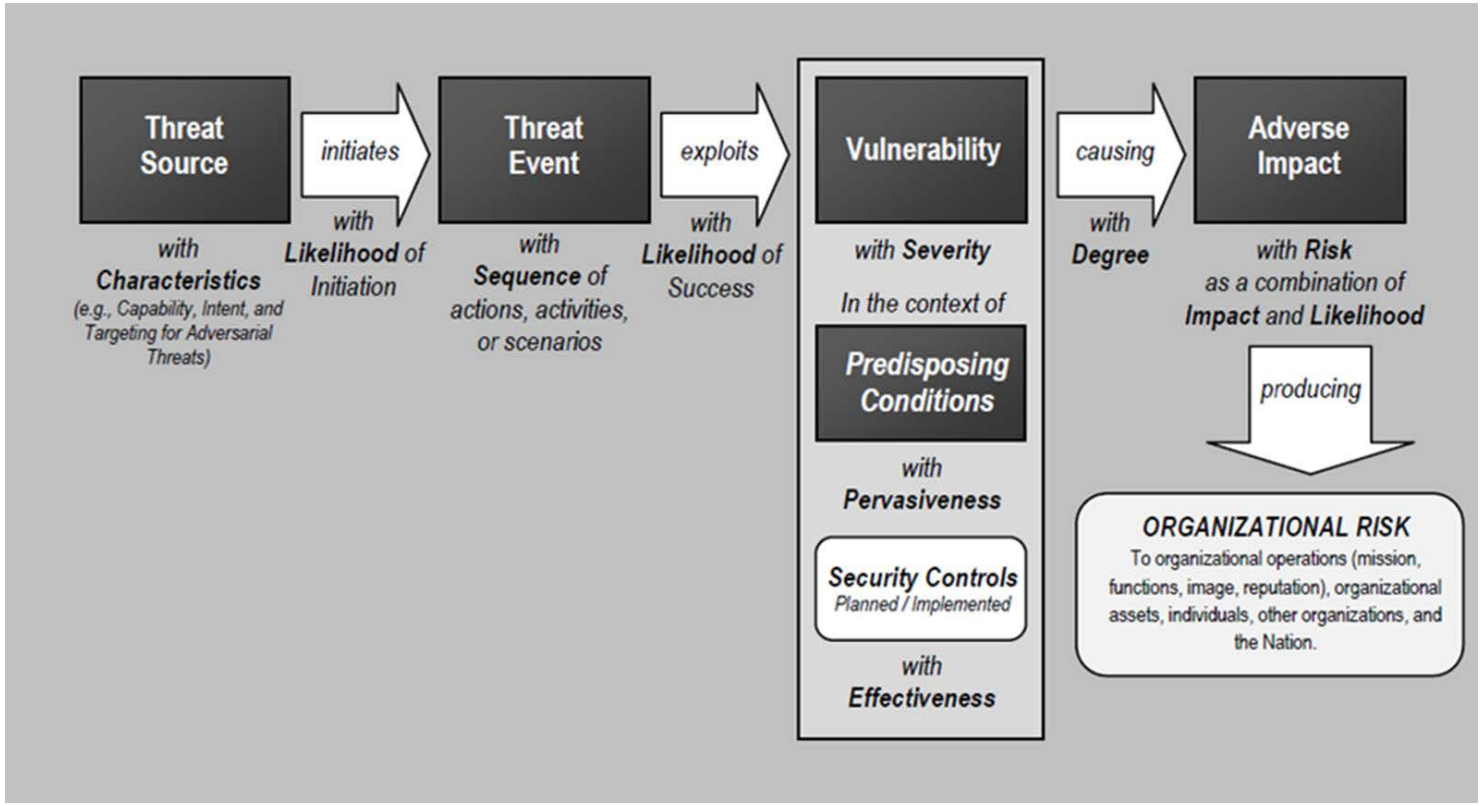
**3. Was Francesco correct or mistaken in his use of the term "proprietary" Saunders data" ?**

**4. Specifically, how does RIT's Information Classifications (Appendix F) relate to this case study scenario?**

## 5. *Who else at RIT would be concerned with this stolen laptop incident?*

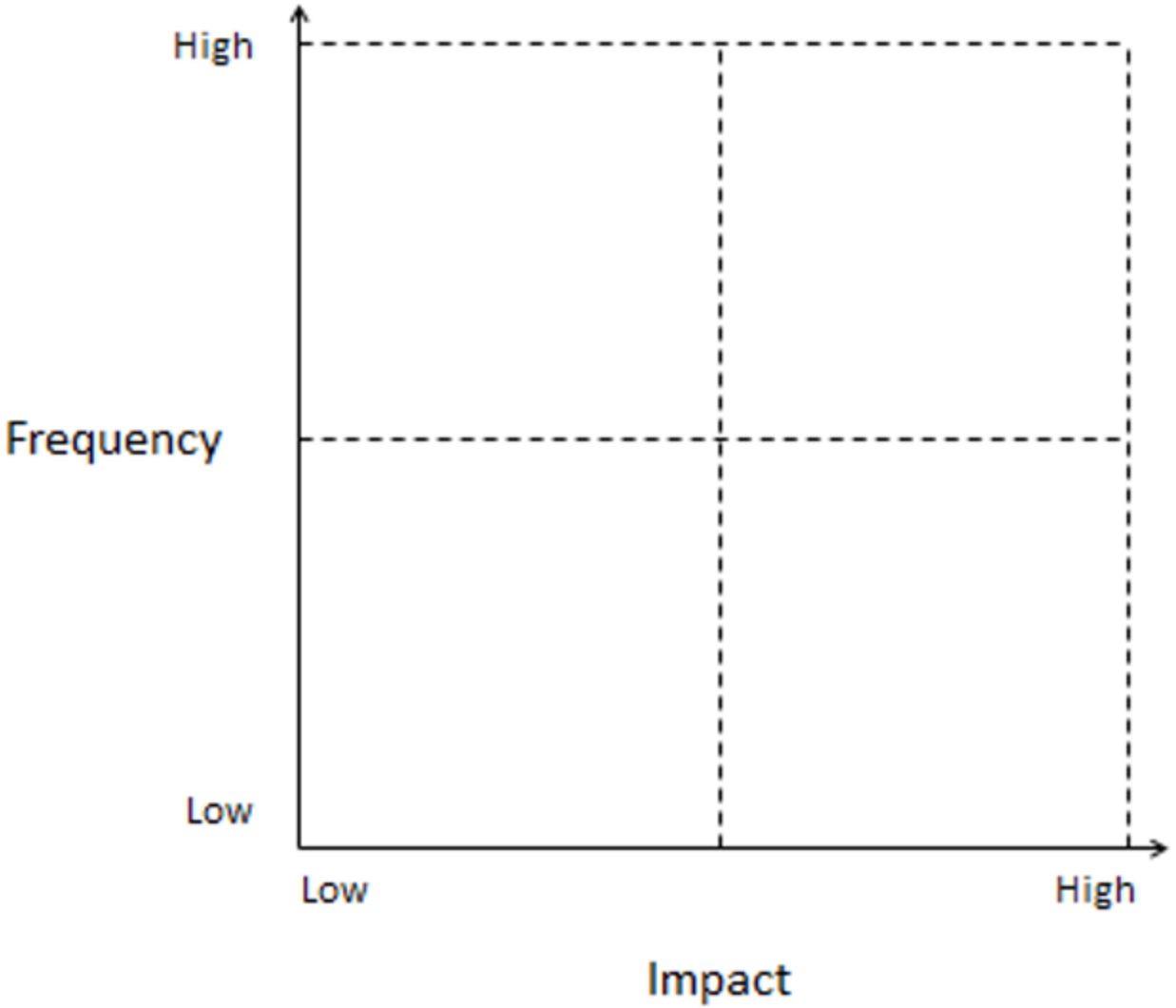
## 6. *Select a stakeholder, analyze this person's concerns about the Dean's lost laptop using this model:*

A. Threat source characteristics
   i. Capability
   ii. Intent
   iii. Targeting
B. Threat event
   i. Attack type
   ii. Likelihood of attack initiation
C. Vulnerability
   i. Weakness type
   ii. Likelihood attack succeeds
D. Impact
   i. Impact type
   ii. Severity of impact
   iii. Overall likelihood
E. Risk



# 7. Organize and present the risks

| Risk | Impact | Frequency |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |






Case Study Analysis: “Snowfall and a stolen laptop”

8. What evidence is the basis for ISO's conclusion that the Dean's stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff?

9. Is the ISO's conclusion valid? Why or why not?

10. What would be the stolen laptop's additional impact on RIT if the ISO's conclusion is not valid ?

# Case Study epilogue and wrap-up

Rochester Institute of Technology (RIT)


Saunders College of Business

Ashok Rao

Janis Gogan • 3rd

Professor at Bentley U and President at Cases for Action

Bentley University • Harvard University

Greater Boston Area • 274