Journal of Information Systems Education

Volume 32
Issue 2
Spring 2021

Teaching Case

Making the Grade: Using COBIT to Study Computer Crime at Bucks County Community College (Pennsylvania)

M. Elizabeth Haywood

Recommended Citation: Haywood, M. E. (2021). Teaching Case: Making the Grade: Using COBIT to Study Computer Crime at Bucks County Community College (Pennsylvania). *Journal of Information Systems Education*, 32(2), 115-118.

Article Link: https://jise.org/Volume32/n2/JISE2021v32n2pp115-118.html

Initial Submission:	7 January 2020
Accepted:	3 December 2020
Abstract Posted Online:	13 March 2021
Published:	9 July 2021

Full terms and conditions of access and use, archived papers, submission instructions, a search tool, and much more can be found on the JISE website: http://jise.org

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Teaching Case
Making the Grade: Using COBIT to Study Computer Crime at Bucks County Community College (Pennsylvania)

M. Elizabeth Haywood
Norm Brodsky College of Business
Rider University
Lawrenceville, NJ 08648, USA
msullivan@rider.edu

ABSTRACT

ISACA, a non-profit, independent association that advocates for professionals involved in information security, assurance, risk management, and governance, recently updated its IT governance framework, Control Objectives for Information and Related Technology (COBIT). COBIT 2019 presents a logical approach to information technology and policy issues. Using a recent real-world computer crime that occurred at a community college, students address breaches of various COBIT components. Students then recommend approaches to minimize the risks and vulnerabilities that expose this school and others. This current case familiarizes students with COBIT's components and the value it provides.

Keywords: Case study, Cybersecurity, Framework, Information assurance & security

1. CASE SUMMARY

Using a recent real-world computer crimes case that occurred at a community college, students address aspects of COBIT to evaluate information technology governance and management. Students then recommend approaches to minimize the risks and vulnerabilities that expose this school and others.

2. CASE TEXT

2.1 Premeditation at the Mall[i]

Click, click, click, click tapped the heels of the two women's shoes on the mall's marble floor. The mall was air-conditioned on that hot July day. Shopping really had not been on Suzy Student's (name changed[ii]) mind though as she walked with her friend, Mary Accomplice.

Mary asked Suzy what was the matter as she sensed her friend was abnormally quiet.

Suzy was stressed as she was struggling in her summer microbiology class at the local community college. Suzy contemplated finding a way to change her grades… but without studying. This would violate the *Academic Integrity Policy*[iii] and *Code of Conduct Policy*[iii] at her school, but cracking her professor's password to his gradebook seemed more palatable. Suzy asked Mary for help.

Mary was confused. While she worked as an administrative assistant in radiology at a local medical clinic, she did not have the knowledge to assist with biology topics. She also did not possess hacking skills to break into a computer system. Mary wondered how she could help.

Suzy explained that her instructor, Professor Microbiology, lived locally and may have been a patient at the medical clinic. Suzy asked, "Can you see if this guy has gone to your work or come into your work?" Mary asked why.

Suzy stated she had been to his office multiple times before class for extra help and observed his computer login ended in 161. She had tried to guess his password several times but had been unsuccessful. She had even attempted to use the "change my password" feature in the college's system, but realized she needed the last four digits of the professor's social security number.

Mary wondered about the username. Suzy cleared that up. The college configured its IT infrastructure where faculty and staff's usernames are the same for all systems: it is the last name and their first initial, up to 8 characters. Guessing the username was simple. However, if someone did forget the username, it could be retrieved by entering either the Social Security Number (SSN) or the college ID number and last name.

2.2 Profile and Password Manager

Information on the college's website (*Catalog Information*[iii], *E-Resources Page*[iii], and the *Login Resources Page*[iii]) openly detailed how to set up and/or change a faculty or staff's password. To set up the account initially, one needed the person's username and the last four digits of the person's SSN. In the setup, the program asked for security questions and gave many options from which to choose. Examples were: "What is your mother's maiden name?" "What is the name of your favorite childhood friend?" and "In what city or town was your first job?"

To validate the user's identity, the person needed to re-enter the username, last four digits of the SSN, and his or her birthdate. Then, one of the security questions appeared and the person needed to answer it identically to how it was entered originally. The user then could choose a password that met the following requirements:

- Cannot contain any part of the username, full name, or date of birth.
- Must be a minimum of 8 characters in length and a maximum of 14 characters.
- Must contain both uppercase and lowercase letters.
- Must contain at least one number.
- Must be a new password, not a previously used one.
- (The college's website states that it enforces changing of a password every 180 days.)

When the account holder changed his or her password, the Password Manager alerted the user that it had been updated.

The college's *Electronics Communications Policy*[iii] describes appropriate and inappropriate use of electronic resources, monitoring and confidentiality, reporting misuse, consequences of failure to comply with guidelines for responsible use, and email user responsibilities.

Once in possession of a valid username and password, a user could access many of the college's systems, such as email, the learning platform for courses, registration and billing.

2.3 Identity Theft

Later, Suzy texted Mary. "Has Prof. Microbiology ever been a patient?"

Mary wrote back that she would check the next day.

Indeed, the next day Suzy's phone buzzed. It was from Mary! It read, "This guy?"

Her text included a photo of Professor Microbiology's personal information - his partial social security number, date of birth, address, and mother's maiden name. Suzy immediately recognized the name! It was him!

Suzy texted back that it was the correct person.

"Don't do anything!" Mary shot back. "I could lose my job!"

Suzy did not do anything with that information right away but she kept the idea in the back of her mind.

2.4 Computer Crime

Professor Microbiology's password met the conditions of the college's password requirements as it contained one upper-case letter, one lower-case letter, and at least one numeral. It was also something obscure that only had meaning to him. However, Suzy eventually cracked the password. ***How do you think she did it?*** [iv]

Sitting alone behind her computer, Suzy not only changed her own grades but also the grades of 37 other students in two different microbiology classes. The jarring image of opening the gradebook and finding atypical scores for ALL of his students led Professor Microbiology to alert the administration.

2.5 Investigation and Confession

2.5.1 Suzy's confession. On July 27, 2017, a local township police sergeant traveled to the community college for the report of a computer crime. The sergeant had learned that someone had accessed a faculty's computerized gradebook and changed the grades of 38 students in two different microbiology classes by using the professor's personal and private username and password.

Prof. Microbiology explained to the police officer that he had not given anyone permission to access or alter the grades using the faculty credentials. The sergeant then examined the grade changes and retrieved the IP address records, uncovering a suspect: Suzy Student. Suzy had accessed Prof. Microbiology's faculty account and changed the grades with the same IP address she used to access her own student account and exam scores.

Almost one week later, Suzy, in the presence of her attorney, confessed to accessing the grades under the identity of her microbiology professor, without his permission, and changing her grade and 37 other students' grades.

One question remained unanswered for the sergeant: how had Mary benefitted from helping Suzy? Suzy replied that Mary had not benefitted in any way. Mary had not even known Prof. Microbiology.

The sergeant summed it up. "This was a roll of the dice" as far as whether Prof. Microbiology was a patient.

Suzy answered, "Yes, yes, I wish he was not."

2.5.2 Mary's confession. After Suzy's confession, the sergeant visited Mary at the medical center. Mary voluntarily spoke with the sergeant after he explained he was investigating Suzy for changing her grades at her college.

Mary initially denied providing any of Prof. Microbiology's personal information to Suzy. Then, Mary exclaimed, "I told her not to do it!"

When the sergeant asked Mary if she had sent a screenshot of Prof. Microbiology's personal information to Suzy, Mary asked, "Do I need an attorney?" The sergeant replied that it was her choice. Mary then ended the interview.

2.6 Search Warrant

Four days after the confessions, the sergeant served a search warrant at the medical center seeking records pertaining to Mary's access of Prof. Microbiology's medical records. He obtained computer screen captures of Mary's access.

With this evidence, the sergeant obtained arrest warrants for Suzy Student and Mary Accomplice.

2.7 Aftermath

According to the Court of Common Pleas Criminal Dockets[v], both Suzy and Mary were convicted of identity theft, unlawful use of a computer by accessing it to disrupt functions, and computer trespassing by altering data. Suzy was sentenced to 12 months incarceration but served her sentence through 100 hours of community service. Interestingly, Mary was sentenced to 24 months incarceration but served her sentence through 200 hours of community service. After both Suzy and Mary appeared in court and served their sentences, they requested that their felony convictions be reduced to misdemeanors, and both paid fees to have these criminal cases expunged (Pickul, 2018). However, details about their crimes, sentencing, and tarnished reputations still linger on the Internet and cannot be removed.

3. ASSIGNMENT

1. Consider the seven interacting components of COBIT 2019's Governance system. Describe how the breakdown in at least five of these components contributed to the crimes noted in the case. Make sure to use specific examples from the case to support your answer. Table 1 below can serve as a checklist when composing your answer.
2. Considering your answer in Question 1, provide at least five recommendations to improve IT governance and management at this college (or other colleges/universities with similar policies and procedures).

4. CONCLUSION

Bucks County Community College is not the only college or university that has experienced students breaking into instructors' gradebooks and changing grades. Since 2013, Purdue University, Kennesaw State University, the University of Georgia, and Rhodes College have all faced similar types of computer crimes, evidencing flaws in their IT infrastructure. Since then, these schools, like Bucks County Community College, have altered certain policies and procedures to prevent and mitigate such recurrences. By understanding and applying the interrelated elements of IT governance frameworks such as COBIT as reflected in this case, students can methodically help govern their future employers' IT environments.

5. CASE ENDNOTES

[i] The author only conjectures how conversations actually unfolded relating to these chain of events. Parts of the conversation can be found in the police report and are used in quotes in the description above.

[ii] The names of the suspects and victim have been changed. However, the police criminal complaint and local news stories are public records.

[iii] The author has included pertinent information from these policies into the case narrative. However, anyone wanting additional guidance can access these policies through the links in the reference section. Please note that the college has updated some of these policies since the incident.

[iv] It is not clear in the police report as to exactly how she determined the password. According to the news story (Fox 43 News, 2017) as well as others (i.e., Pickul, 2018), it appears that she used the information she gained from her friend. However, another theory on how Suzy cracked the password was that a phone or other device could have captured the professor's keylogging strokes. This highlights the importance of protecting passwords in the presence of others.

[v] Court of Common Pleas of Bucks County Criminal Docket Numbers (2017). CP-09-CR-0007789-2017 and CP-09-CR-0008474-2017.

Choose five from the following COBIT IT Governance Framework Components:	**COBIT Component**	**Case Example**
Processes *describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.*		
Organizational structures *are the key decision-making entities in an enterprise.*		
Principles, policies, and frameworks *translate desired behavior into practical guidance for day-to-day management.*		
Information *is pervasive throughout any organization and includes all information produced and used by the enterprise. COBIT focuses on the information required for the effective functioning of the governance system of the enterprise.*		
Culture, ethics, and behavior *of individuals and of the enterprise are often underestimated as factors in the success of governance and management objectives.*		
People, skills, and competencies *are required for good decisions, execution of corrective action and successful completion of all activities.*		
Services, infrastructure, and applications *include the infrastructure, technology and applications that provide the enterprise with the governance system for I&T processing.*		

Table 1. Guidance for Formulating Answers

6. REFERENCES

Bucks County Community College Academic Integrity Policy (2018). Retrieved March 15, 2018, from http://www.bucks.edu/policy/academicintegrity/.

Bucks County Community College Catalog Information (2018). Retrieved March 15, 2018, from http://www.bucks.edu/catalog/info/records/communications/.

Bucks County Community College Code of Conduct (2018). Retrieved March 15, 2018, from http://www.bucks.edu/policy/codeofconduct/.

Bucks County Community College E-Resources Page (2018). Retrieved March 15, 2018, from http://www.bucks.edu/policy/e-resources/password/.

Bucks County Community College Electronic Communications Policy (2018). Retrieved March 15, 2018, from https://www.bucks.edu/catalog/info/records/ecommunications/.

Bucks County Community College Login Resources Page (2018). Retrieved March 15, 2018, from http://www.bucks.edu/resources/it/logins/staff/.

Commonwealth of Pennsylvania, County of Bucks, Police Criminal Complaint 20170726M8196 filed November 16, 2017.

Court of Common Pleas of Bucks County Criminal Docket Numbers (2017). CP-09-CR-0007789-2017 and CP-09-CR-0008474-2017.

Fox 43 News - York. (2017). Bucks County Women Accused of Conspiring to Hack into Community College Computer System to Change Grades. Retrieved March 15, 2018, from (http://fox43.com/2017/11/16/bucks-county-women-accused-of-conspiring-to-hack-into-community-college-computer-system-to-change-grades/.

Pickul, M. (2018). Update in Bucks Hacking Scandal. *The Centurion (The Student Newspaper of Bucks County Community* College). Retrieved October 29, 2020, from https://www.bucks-news.com/news/2018/10/04/update-in-bucks-hacking-scandal/.

AUTHOR BIOGRAPHY

M. Elizabeth "Betsy" Haywood is an associate professor of accounting at the Norm Brodsky College of Business at Rider University. Her Ph.D. is from the University of Georgia. Her work has appeared in *Issues in Accounting Education*, *Journal of Accounting Education*, *Advances in Accounting Education, Strategic Finance, Management Accounting Quarterly, Accounting Instructor's Report,* as well as others.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©2021 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, Journal of Information Systems Education, editor@jise.org.

ISSN 2574-3872