https://doi.org/10.48009/4_iis_2020_168-177

Issues in Information Systems
Volume 21, Issue 4, pp. 168-177, 2020

INFORMATION SYSTEMS SECURITY EDUCATION: MIS MAJORS AND BUSINESS MAJORS IN AACSB COLLEGE OF BUSINESSES

Kevin Lee Elder, MIS, Georgia College & State University, Kevin.Elder@GCSU.edu
Thomas S. E. Hilton, Information Systems, University of Wisconsin–Eau Claire, HiltonTS@uwec.edu

ABSTRACT

This a follow-on to previous IACIS 2018 & 2019 presentations that reported on a needs analysis of information systems security education at a 2,500-student college of business in an 11,000-student university in the Upper Midwest USA (UWEC). This year we bring in some results from a 1,700-student college of business in a 6,500-student university in the Southeast USA (GCSU). Preliminary Results are summarized in tables 1 and 2. In this study we compare MIS majors and Business Students and find little differences and conclude much more research is needed. Security of information systems is becoming more crucial by the day (Cerrudo, 2017), both conceptual knowledge and skill in tool use being necessary (Tarala, 2011). Countering this trend is the growing perception that young adults preparing to enter the work force are increasingly uninformed about basic endpoint security concepts and tools (Schaffhauser, 2015). This is counterintuitive given the widely assumed familiarity with information technology of contemporary young adults (Anderson & Rainie, 2012).

Keywords: Cyber Security, Security Education, AACSB Institutions, Security Tools, Security Skills

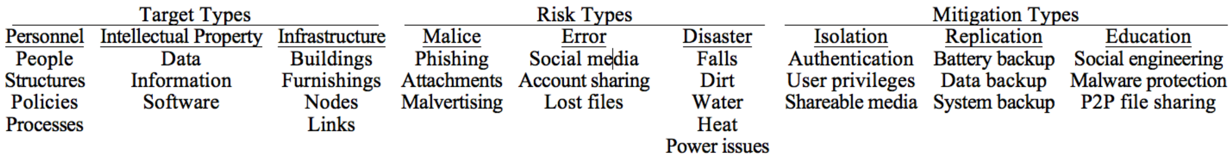
INTRODUCTION

2018 Study Description

Endpoint security is securing the laptops or desktops, and other networked computing devices used by professionals who, though presumably expert in their fields, are not primarily employed to secure information technology (Lord, 2017). The first study in s multi-part series aimed to establish a baseline of endpoint security knowledge and skill among young-adult business majors at an upper Midwest university (University of Wisconsin–Eau Claire). A self-report survey was administered to approximately 800 business majors, mostly sophomores and juniors, in the business-core information systems course. The aim was to guide curriculum development to effectively target areas where instruction and practice are needed (Hilton, 2018).

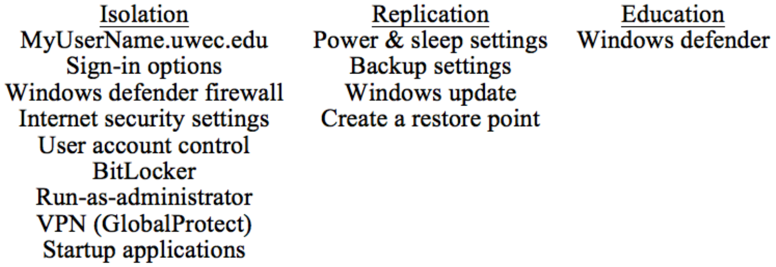
Instructors from all major programs in the College of Business (accounting, finance, information systems, management, and marketing) as well as members of the university's administrative computing group were interviewed to describe concepts and tools they regard as particularly important for students. Tables 1 and 2 organize the content areas thus identified by target type, risk type, and mitigation type (Hilton 2018):

Table 1. Desirable End-Point Security Concepts



Target Types			Risk Types			Mitigation Types		
Personnel	Intellectual Property	Infrastructure	Malice	Error	Disaster	Isolation	Replication	Education
People	Data	Buildings	Phishing	Social media	Falls	Authentication	Battery backup	Social engineering
Structures	Information	Furnishings	Attachments	Account sharing	Dirt	User privileges	Data backup	Malware protection
Policies	Software	Nodes	Malvertising	Lost files	Water	Shareable media	System backup	P2P file sharing
Processes		Links			Heat			
					Power issues			

Table 2. Desirable Windows 10 End-Point Security Tools

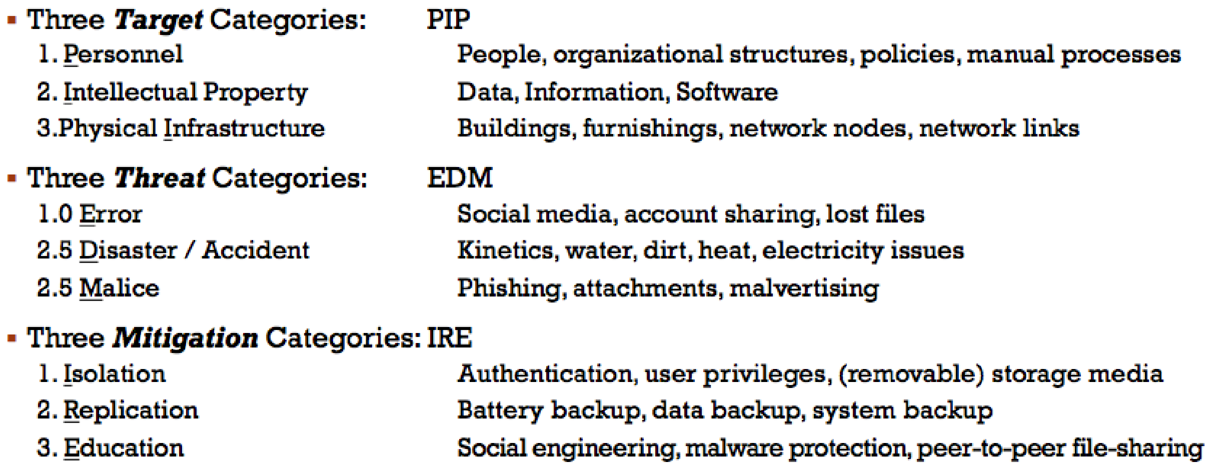


Isolation	Replication	Education
MyUserName.uwec.edu	Power & sleep settings	Windows defender
Sign-in options	Backup settings	
Windows defender firewall	Windows update	
Internet security settings	Create a restore point	
User account control		
BitLocker		
Run-as-administrator		
VPN (GlobalProtect)		
Startup applications		

Prioritized *Concept* Model of Observations

The model developed to create an instructional unit for the education of students was built on the "Three Threes" of Information Assurance as shown in Table 3.

Table 3. "Three Threes" of Information Assurance



▪ Three ***Target*** Categories:	PIP
1. Personnel	People, organizational structures, policies, manual processes
2. Intellectual Property	Data, Information, Software
3.Physical Infrastructure	Buildings, furnishings, network nodes, network links
▪ Three ***Threat*** Categories:	EDM
1.0 Error	Social media, account sharing, lost files
2.5 Disaster / Accident	Kinetics, water, dirt, heat, electricity issues
2.5 Malice	Phishing, attachments, malvertising
▪ Three ***Mitigation*** Categories:	IRE
1. Isolation	Authentication, user privileges, (removable) storage media
2. Replication	Battery backup, data backup, system backup
3. Education	Social engineering, malware protection, peer-to-peer file-sharing

Students were then surveyed to determine their reported competencies. Results are shown in Figure 1 and Table 4. There was a very high response rate, section 1 had 97.84% rate and section 2 had a 92.75% rate. There was close agreement between the two sections. A Likert scale of 1 to 5 was used. Overall average responses were almost exactly at the midpoint (3.06). Most of the student's responses were at or below the midpoint of responses. Most students were giving "expected" responses. Not unexpected was the fact students were less confident in skills than they were of their knowledge of these concepts. Most respondents were not confident in their knowledge, while a few were very confident. Students knew very little about BitLocker as it had the lowest response mean. The Power & Sleep settings had the highest response mean, almost all students have set those. The greatest spread in response means was for the tools. All three tools shown in green in the top part of Table 4 were things Windows forces on users so it is no surprise that those were the most highly rated.

Therefore, this survey and the interviews of faculty, students and staff can be used in the creation of an instructional unit for students to complete to test their knowledge and ability to update their own computers for proper cyber security in future research projects.

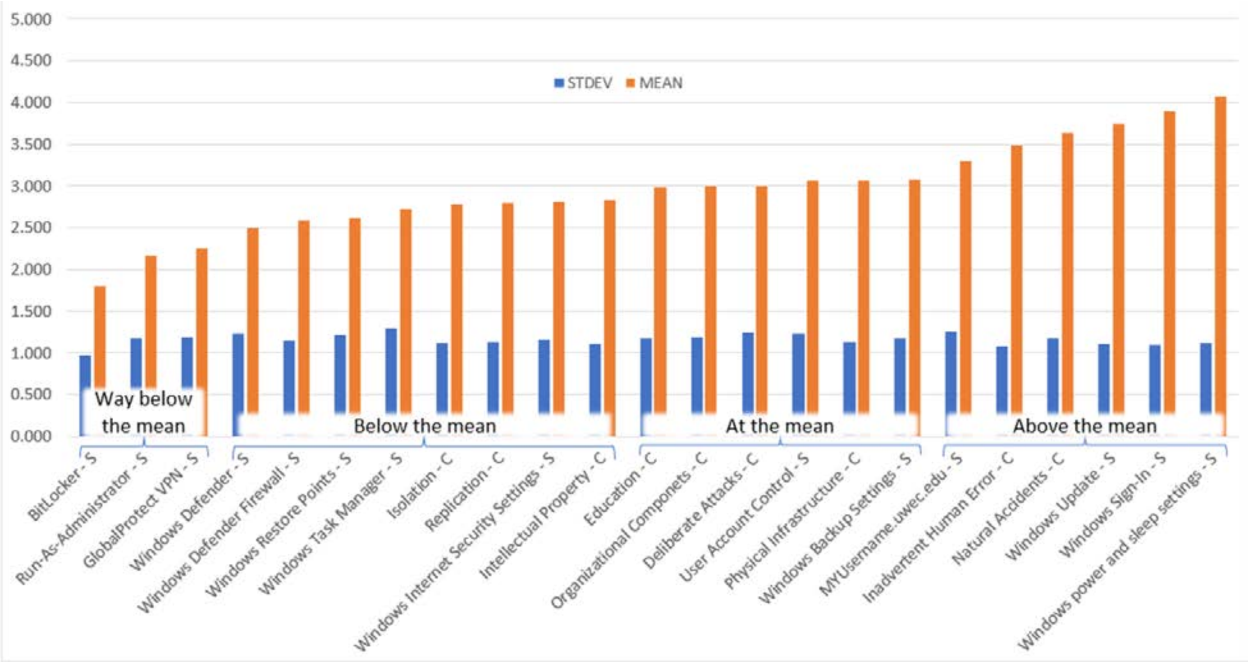
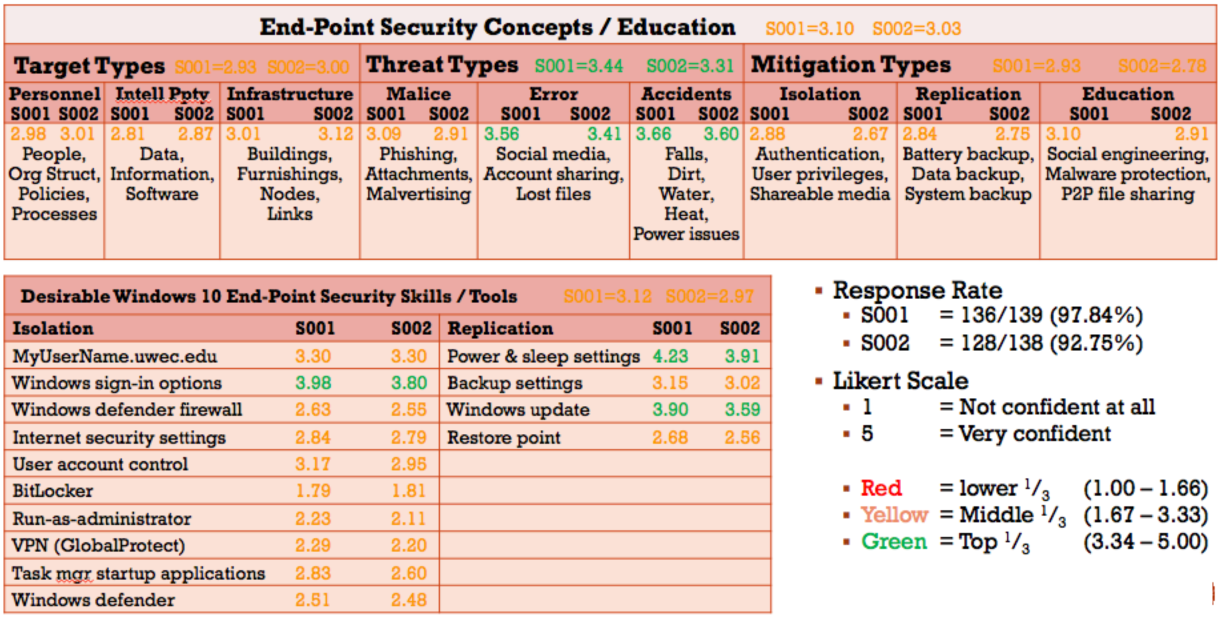


Figure 1. Reported Competencies in Tools

Table 4. Reported Competencies: Student Surveys



End-Point Security Concepts / Education S001=3.10 S002=3.03																	
Target Types S001=2.93 S002=3.00						Threat Types S001=3.44 S002=3.31						Mitigation Types S001=2.93 S002=2.78					
Personnel		Intell Ppty		Infrastructure		Malice		Error		Accidents		Isolation		Replication		Education	
S001	S002	S001	S002	S001	S002	S001	S002	S001	S002	S001	S002	S001	S002	S001	S002	S001	S002
2.98	3.01	2.81	2.87	3.01	3.12	3.09	2.91	3.56	3.41	3.66	3.60	2.88	2.67	2.84	2.75	3.10	2.91
People, Org Struct, Policies, Processes		Data, Information, Software		Buildings, Furnishings, Nodes, Links		Phishing, Attachments, Malvertising		Social media, Account sharing, Lost files		Falls, Dirt, Water, Heat, Power issues		Authentication, User privileges, Shareable media		Battery backup, Data backup, System backup		Social engineering, Malware protection, P2P file sharing	

Desirable Windows 10 End-Point Security Skills / Tools S001=3.12 S002=2.97					
Isolation	**S001**	**S002**	**Replication**	**S001**	**S002**
MyUserName.uwec.edu	3.30	3.30	Power & sleep settings	4.23	3.91
Windows sign-in options	3.98	3.80	Backup settings	3.15	3.02
Windows defender firewall	2.63	2.55	Windows update	3.90	3.59
Internet security settings	2.84	2.79	Restore point	2.68	2.56
User account control	3.17	2.95			
BitLocker	1.79	1.81			
Run-as-administrator	2.23	2.11			
VPN (GlobalProtect)	2.29	2.20			
Task mgr startup applications	2.83	2.60			
Windows defender	2.51	2.48			

- Response Rate
  - S001 = 136/139 (97.84%)
  - S002 = 128/138 (92.75%)
- Likert Scale
  - 1 = Not confident at all
  - 5 = Very confident

  - Red = lower $^1/_3$ (1.00 – 1.66)
  - Yellow = Middle $^1/_3$ (1.67 – 3.33)
  - Green = Top $^1/_3$ (3.34 – 5.00)

2018 Industry Implications

The implications for the IT industry and for the economy at large are significant since employee error is universally recognized as the common denominator in all information security breaches (Tarala, 2011). Great risk attends the graduating of business professionals who do not engage in reasonable security practices with their endpoint computing devices. Interestingly, the interviews with instructors and computing professionals yielded some results that surprised this researcher. First, more than twice as many concepts as skills were identified; evidently knowing about security is of greater concern than actually using security tools. Second, the great majority of tools are for isolation, as opposed to replication or education. Third, the anti-malware tool most favored (by interviewees who had an opinion) was Microsoft Windows Defender; this is curious since Windows Defender is almost invisible in anti-malware product reviews (Rubenking, 2018; Tung, 2018).

2019 Study Description:

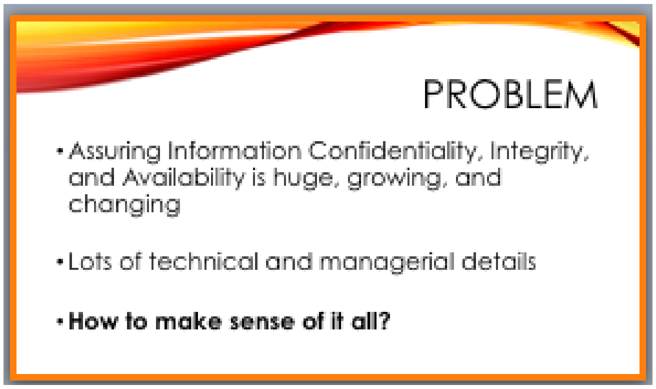
This study chronicled the development of an instructional unit for all business students that addresses the information systems security concepts and skills identified by Hilton (2018). Obstacles and techniques to address them are detailed:

Stakeholder Acceptance:	Student	(Fatalism)
	Instructor	(Territoriality)
	Administrator	(AACSB)
	Campus Computing	(Distraction)
Development Resource Availability:	Staff	(Campus v. Online)
	Time	(Summer)
	Funding	(Summer)
	Course	(IS, BCOM, ACCT)
Delivery Resource Availability:	Content	(Theory v. Practice)
	Hardware	(Windows v. Mac)
	Software	(Licensing)

Wallace (2015) states, “with countless threats and limited budgets, organizations can’t eliminate all risks and must make careful assessments to manage them.” According to Cabaj et al. (2018), cybersecurity is considered an independent discipline. It is a “computing based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries” and involves the creation, operation, analysis, and testing of secure computer systems; and also includes aspects of law, policy, human factors, ethics, and risk management (Cabaj et al., 2018). Therefore, higher education institutions must respond and besides offering degree programs to meet newfound demands they must educate all majors on some of the most prominent information for end users to know about cyber security. Even in the Dental Healthcare Industry Melon and Hernandez (2018) found that practitioners need to integrate a plan of recurrent updates of all devices' software, including operating systems (Lisbon, 2018) and frequently user awareness training to review the practices and new trends (Sabillon, Cavaller & Cano, 2016). It is important to integrate of information technology training (IT) (Hoffman, Burley & Toregas, 2011; Scarbecz & DeSchepper, 2018) with devices and information systems in the office.

Creation of the PowerPoint Deck and Assignment

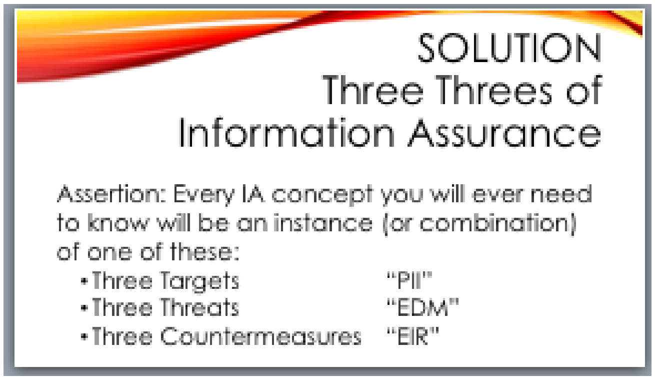
From the 2018 and 2019 studies a PowerPoint deck explaining The Three Threes of Information Assurance was created along with the assignment as partially shown in Figures 2, 3, 4 and 5. It was built off the data and results from the previous two projects with the hopes of collecting more data.



PROBLEM

- Assuring Information Confidentiality, Integrity, and Availability is huge, growing, and changing
- Lots of technical and managerial details
- **How to make sense of it all?**

Figure 2. Assignment PowerPoint Deck Problem

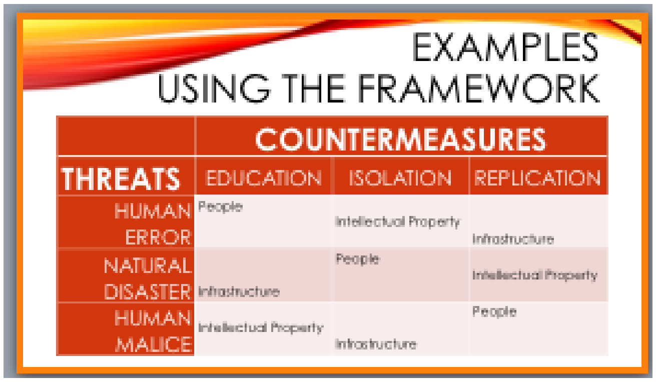


SOLUTION
Three Threes of
Information Assurance

Assertion: Every IA concept you will ever need to know will be an instance (or combination) of one of these:

- Three Targets "PII"
- Three Threats "EDM"
- Three Countermeasures "EIR"

Figure 3. Assignment PowerPoint Deck Solution



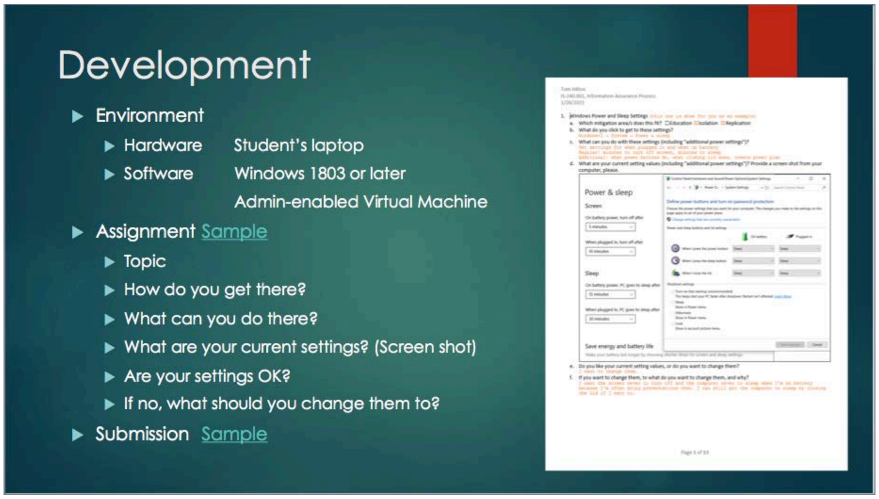
EXAMPLES
USING THE FRAMEWORK

	COUNTERMEASURES		
THREATS	EDUCATION	ISOLATION	REPLICATION
HUMAN ERROR	People	Intellectual Property	Infrastructure
NATURAL DISASTER	Infrastructure	People	Intellectual Property
HUMAN MALICE	Intellectual Property	Infrastructure	People

Figure 4. Assignment PowerPoint Deck Framework Explanation

The aim of the assignment was to teach students to "Protect targets against threats via mitigations." The three targets are, People, Intellectual Property and Infrastructure. The three threat areas are, Error, Disaster and Malice. The three mitigation areas are, Education, Isolation and Replication. Two skill areas are, End Users and Windows.

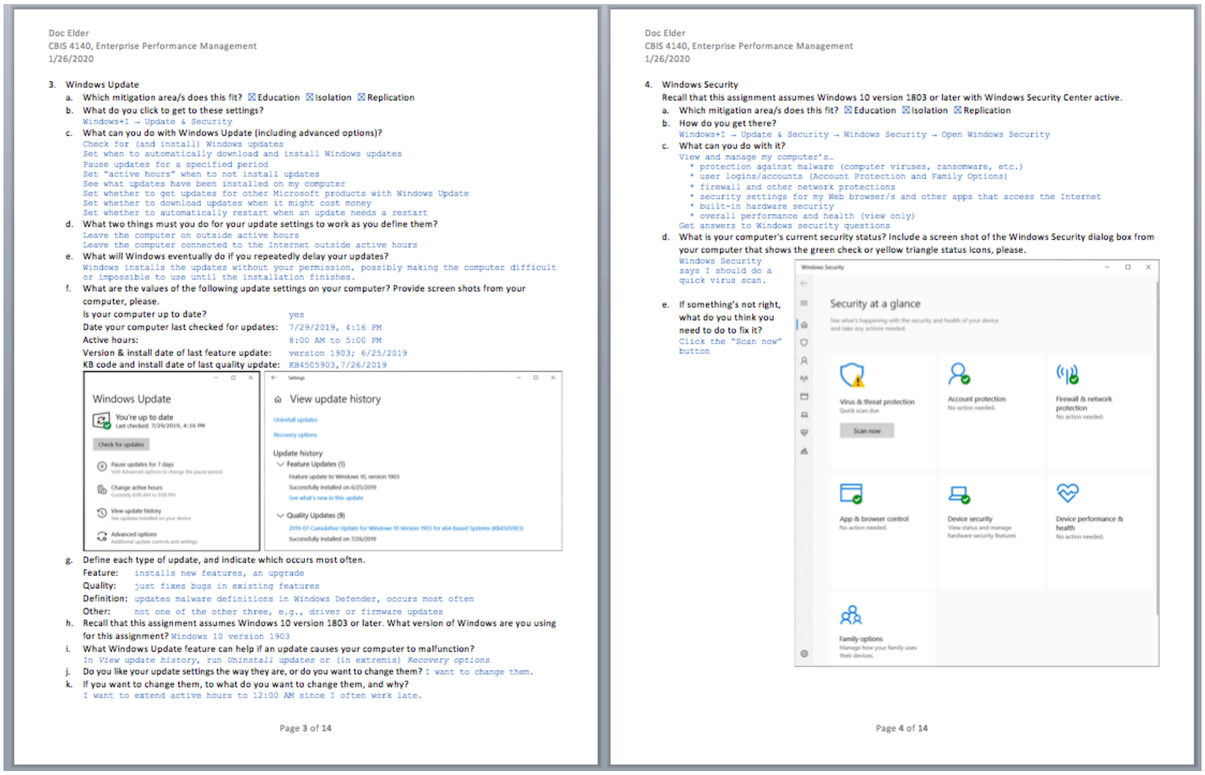
The assignment was developed and administered at the University of Wisconsin–Eau Claire in the Fall of 2019 and at the second college in the Spring of 2020. The students were given the assignment, the PowerPoint deck with explanation of the theory and framework as shown above in figures 2, 3, and 4 and guidelines and example as partially shown in Figure 5 and 6.



Development

- Environment
  - Hardware — Student's laptop
  - Software — Windows 1803 or later
Admin-enabled Virtual Machine
- Assignment Sample
  - Topic
  - How do you get there?
  - What can you do there?
  - What are your current settings? (Screen shot)
  - Are your settings OK?
  - If no, what should you change them to?
- Submission Sample

Figure 5. Assignment Development Guidelines and Example



Doc Elder
CBIS 4140, Enterprise Performance Management
1/26/2020

3. Windows Update
   a. Which mitigation area/s does this fit? ☒ Education ☒ Isolation ☒ Replication
   b. What do you click to get to these settings?
   Windows+I → Update & Security
   c. What can you do with Windows Update (including advanced options)?
   Check for (and install) Windows updates
   Set when to automatically download and install Windows updates
   Pause updates for a specified period
   Set "active hours" when to not install updates
   See what updates have been installed on my computer
   Set whether to get updates for other Microsoft products with Windows Update
   Set whether to download updates when it might cost money
   Set whether to automatically restart when an update needs a restart
   d. What two things must you do for your update settings to work as you define them?
   Leave the computer on outside active hours
   Leave the computer connected to the Internet outside active hours
   e. What will Windows eventually do if you repeatedly delay your updates?
   Windows installs the updates without your permission, possibly making the computer difficult or impossible to use until the installation finishes.
   f. What are the values of the following update settings on your computer? Provide screen shots from your computer, please.

Is your computer up to date?	yes
Date your computer last checked for updates:	7/29/2019, 4:16 PM
Active hours:	8:00 AM to 5:00 PM
Version & install date of last feature update:	version 1903; 6/25/2019
KB code and install date of last quality update:	KB4505903,7/26/2019

Windows Update
You're up to date
Last checked: 7/29/2019, 4:16 PM
Check for updates
Pause updates for 7 days
Visit Advanced options to change the pause period
Change active hours
Currently 8:00 AM to 5:00 PM
View update history
See updates installed on your device
Advanced options
Additional update controls and settings

Settings
View update history
Uninstall updates
Recovery options
Update history
Feature Updates (1)
Feature update to Windows 10, version 1903
Successfully installed on 6/25/2019
See what's new in this update
Quality Updates (9)
2019-07 Cumulative Update for Windows 10 Version 1903 for x64-based Systems (KB4505903)
Successfully installed on 7/26/2019

   g. Define each type of update, and indicate which occurs most often.

Feature:	installs new features, an upgrade
Quality:	just fixes bugs in existing features
Definition:	updates malware definitions in Windows Defender, occurs most often
Other:	not one of the other three, e.g., driver or firmware updates

   h. Recall that this assignment assumes Windows 10 version 1803 or later. What version of Windows are you using for this assignment? Windows 10 version 1903
   i. What Windows Update feature can help if an update causes your computer to malfunction?
   In *View update history*, run *Uninstall* updates or (in extremis) *Recovery options*
   j. Do you like your update settings the way they are, or do you want to change them? I want to change them.
   k. If you want to change them, to what do you want to change them, and why?
   I want to extend active hours to 12:00 AM since I often work late.

Page 3 of 14

Doc Elder
CBIS 4140, Enterprise Performance Management
1/26/2020

4. Windows Security
   Recall that this assignment assumes Windows 10 version 1803 or later with Windows Security Center active.
   a. Which mitigation area/s does this fit? ☒ Education ☒ Isolation ☒ Replication
   b. How do you get there?
   Windows+I → Update & Security → Windows Security → Open Windows Security
   c. What can you do with it?
   View and manage my computer's…
   * protection against malware (computer viruses, ransomware, etc.)
   * user logins/accounts (Account Protection and Family Options)
   * firewall and other network protections
   * security settings for my Web browser/s and other apps that access the Internet
   * built-in hardware security
   * overall performance and health (view only)
   Get answers to Windows security questions
   d. What is your computer's current security status? Include a screen shot of the Windows Security dialog box from your computer that shows the green check or yellow triangle status icons, please.
   Windows Security says I should do a quick virus scan.
   e. If something's not right, what do you think you need to do to fix it?
   Click the "Scan now" button

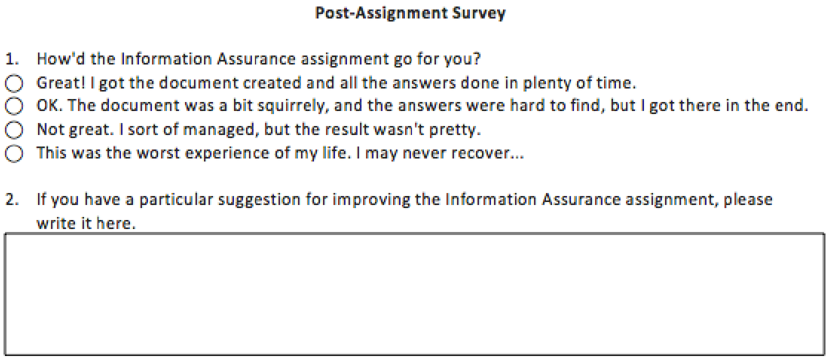
Windows Security
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
Quick scan due
Scan now
Account protection
No action needed.
Firewall & network protection
No action needed.
App & browser control
No action needed.
Device security
View status and manage hardware security features
Device performance & health
No action needed.
Family options
Manage how your family uses their devices.

Page 4 of 14

Figure 6. Assignment Example Pages from GCSU

RESULTS

At the University of Wisconsin–Eau Claire, an Upper Midwest college of business, students in a core IS class for all majors completed the assignment and a post assignment survey with only two questions. As shown in Figure 7, the first survey question had asked how the students felt the assignment had gone, and the second question asked for any suggestions for improvement:



Post-Assignment Survey

1. How'd the Information Assurance assignment go for you?

○ Great! I got the document created and all the answers done in plenty of time.
○ OK. The document was a bit squirrely, and the answers were hard to find, but I got there in the end.
○ Not great. I sort of managed, but the result wasn't pretty.
○ This was the worst experience of my life. I may never recover...

2. If you have a particular suggestion for improving the Information Assurance assignment, please write it here.

Figure 7. Post Assignment Survey

Faculty and staff reviewed the assignment before it was given to students. Faculty responded overwhelmingly that they, the faculty, should complete the assignment since they, the faculty, did not know laptop security either. Staff responded that it was harder than they thought it would be. Then the students completed the assignment. The scores ranged from a low of 20 percent (lower than expected) to a high of 100 percent with an average of 85 (higher than expected).

Results of the Post Assignment Survey are depicted in Figure 8 below. Only 1 in 10 students felt the assignment experience had gone great without taking too much time to complete, which matched the needs assessment results where a small percentage were confident they knew about the topic. Approximately 50 percent of the students felt the assignment had gone okay, with it taking a good amount of time and searching to complete the assignment but still completing it in time. This closely matched up with the average score of 85 on the assignment. However, 25 percent felt the assignment had not been great, they managed to complete the assignment, but they did not have confidence in their answers. Even worse, 14 percent felt the experience was the worst and they may never recover. For the first time out the results were pretty much to be expected. But it would be nice to compare results to another university.

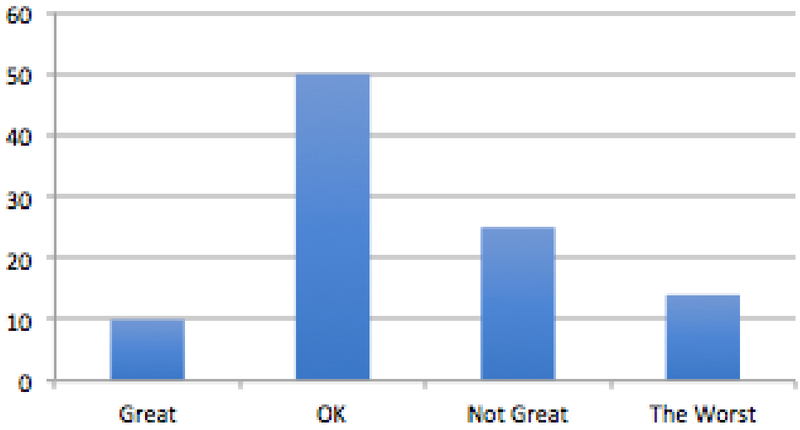


Figure 8. Affect Post-Survey at the University of Wisconsin-Eau Claire

2020 Study Description

At University number 2, a Southeast university college of business (Georgia College & State University), students in an upper level MIS major's class were given the same assignment, with minor changes for the new environment, and the same post assignment survey with only two questions was also administered.

The assignment scores were similar to the first set of data, although since these were MIS majors one would expect the low scores would be higher and they were. The lowest score was a 40 percent, which was twice as high. The Max percent was also a 100 percent, maybe we need to add some extra credit to see if there is a difference on the high end of the cores. The average was only 86.5 percent that was not significantly different from the first data set for any majors. Thus, it can be concluded that all business majors have students that are comfortable with their technology and when faced with security configuration tasks to perform on their laptops there are students in every major that can ace the assignment. The lower end of the majors are different: IT majors are better with laptop security than other majors, but the score was still considered pretty poor for what we are measuring.

The results of the Post Assignment Survey, are depicted in Figure 9 below. Only 1 in 6 students felt the assignment experience had gone great without taking too much time to complete, which was an improvement from University 1, showing there is a little bit larger but still small percentage that were confident they knew about this topic. Approximately 55 percent of the students felt the assignment had gone okay, with it taking a good amount of time and searching to complete the assignment but still completing it in time. This closely matched up with the resulting average of 86.5 on the assignment as was slightly higher than the University of Wisconsin-Eau Claire. Yet both data sets showed a majority of the students once shown what to do are confident with these new skills. However, 14 percent felt the assignment had not been great, they sort of managed to complete the assignment but they did not have confidence in their answers. This was better than the University of Wisconsin-Eau Claire, but you would expect IT majors would have fewer students at the lower levels of affect. But once again 14 percent felt the experience was the worst and they may never recover. This was the same percent as we found in the University of Wisconsin-Eau Claire. Therefore, the bottom of the range of students appears the same for all majors, even IT when it comes to laptop security. For the second time out the results were pretty much to be expected, but it demonstrates much more research is necessary to see if we can move this needle. And it would be nice to compare these results to more universities and more majors.

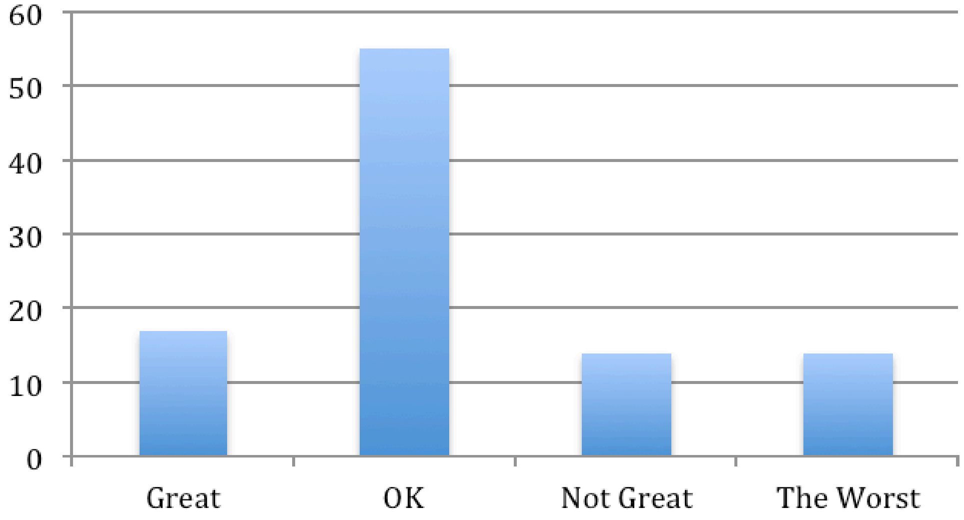


Figure 9. Affect Post-Survey at Georgia College & State University

Results for both Universities can be compared in Figure 10; they are similar.

The implications for the regional IT industry, indeed the entire regional economy, are significant since employee error is universally recognized as the common denominator in all information security breaches. Great risk attends the graduating of business professionals who do not engage in reasonable security practices with their client computing devices.

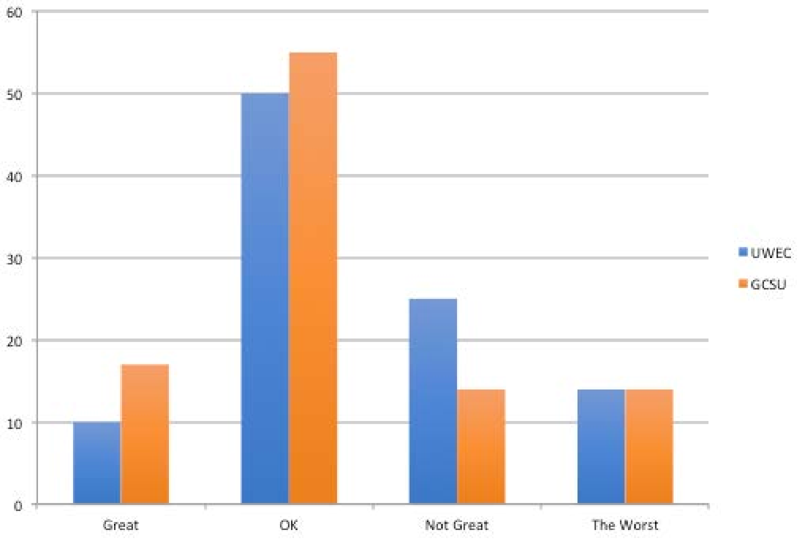


Figure 10. Affect Post-Survey the University of Wisconsin-Eau Claire vs. Georgia College & State University

SUMMARY

Information assurance is complex. A few related principles help tame the complexity. As things change, these concepts remain helpful. Endpoint security is one of the most important things students can learn about technology in a business degree. This assignment is a starting point, but students need to practice secure computing throughout the rest of their courses --and throughout their life. Secure computing entails both concepts and skills, things they need to know and things they need to do. This assignment helps the students move along the path of knowing what they should know and doing what they should do to practice safe computing in the College of Business (and elsewhere).

Common themes emerged that we here group into three domains:

1. Targets are IA objects at risk of having their confidentiality, integrity, or availability harmed.
   a. People: the most important information asset to protect!
   b. Intellectual Property: data, information, and custom software
   c. Physical Infrastructure: computers, cables, desks, rooms, electrical wiring, cooling systems, etc.
2. Threats are methods of harming targets' confidentiality, integrity, or availability.
   a. Human Error: about 2/3 of all IA lapses in the USA each year
   b. Natural Accidents: often called acts of God by insurance companies, about 1/6 of IA lapses in the USA
   c. Human Malice: phishing, viruses, Trojan horses, logic bombs, denial-of-service botnets, ransomware, social engineering, and myriad other malware; about 1/6 of annual IA lapses in the USA
3. Mitigations are methods of minimizing the effects of threats. IA experts usually talk mitigation rather than elimination since, practically speaking, elimination is usually impossible.
   a. Education: courses, assignments, and documentation such as posters, leaflets, handouts, etc.
   b. Isolation: password-protected accounts, electrical surge protectors, firewalls, etc.
   c. Replication: backups of software and data, batteries, cloud-computing, cross-training, etc.

The business process that integrates these "three threes" is known as Information Assurance Risk Management, and its aim is to mitigate threats against targets. We hope more universities will join the project.

REFERENCES

Anderson, J & Rainie, L. (2012). “Main findings: Teens, technology, and human potential in 2020.” Pew Research Center: Internet & Technology. February 29, 2012. Retrieved July 13, 2018 from http://www.pewinternet.org/2012/02/29/main-findings-teens-technology-and-human-potential-in-2020/.

Cerrudo, C. (2017). "Why Cybersecurity should be the biggest concern of 2017." Forbes Magazine. January 17, 2017. Retrieved July 13, 2018 from https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#59359ecc5218.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24-35.

Hilton, T. (2018) "Endpoint Security Knowledge and Skill of Business Undergraduates." Proceedings of the International Association for Computer Information Systems 58th International Conference. October 2018. Retrieved June 1, 2020 from https://iacis.org/conference/proceedings/IACIS_2018_Proceedings.pdf.

Hilton, T. and Staloch, M. (2019) "Information Systems Security in the Core Content of an AACSB College of Business." Proceedings of the International Association for Computer Information Systems 59th International Conference. October 2019. Retrieved June 1, 2020 from https://iacis.org/conference/proceedings/IACIS_2019_Proceedings.

Hoffman, L. J., Burley, D., & Toregas, C. (2011). Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce. IEEE Security and Privacy, 1–13.

Lisbon, S. (2018). A Comparative Analysis of HIPAA Security Risk Assessments for Two Small Dental Clinics. 11– 13.

Lord, N. (2017). "What is endpoint security? Data protection 101." Digital Guardian: Data Insider. July 27, 2017. Retrieved July 13, 2018 from https://digitalguardian.com/blog/what-endpoint-security-data-protection-101.

Melon, E. and Hernandez, W. (2020) "Cybersecurity in the Dental Healthcare Sector: The Need of Knowledge for Small Practioners." Issues in Information Systems, Volume 21, Issue 1, pp. 118-124, 2020.

Rubenking, N. (2018). "The best antivirus protections of 2018." PC Magazine. July 11, 2018. Retrieved July 13, 2018 from https://www.pcmag.com/article2/0,2817,2372364,00.asp.

Rubenking, N. (2018). "The best free antivirus protections of 2018." PC Magazine. April 14, 2018. Retrieved July 13, 2018 from https://www.pcmag.com/article2/0,2817,2388652,00.asp.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering, 5(5), 2409–4285. www.IJCSSE.org

Scarbecz, M., & DeSchepper, E. (2018). Trends in First-Year Dental Students' Information Technology Knowledge and Use: Results from a U.S. Dental School in 2009, 2012, and 2017. Journal of Dental Education, 82(12), 1287–1295.

Schaffhauser, D. (2015). "Report: 6 of 10 millennials have 'low' technology skills." THE Journal. June 11, 2015. Retrieved July 13, 2018 from https://thejournal.com/articles/2015/06/11/report-6-of-10-millennials-have-low-technology-skills.aspx.

Tarala, J. (2011). "Network security: Theory versus practice." SANS Analyst Program. May 2011. Retrieved July 13, 2018 from https://www.sans.org/reading-room/whitepapers/analyst/network-security-theory-practice-35025.

Tung, L. (2018). "Microsoft: Here's why Windows Defender AV isn't ranked higher in new antivirus tests." ZDNet. May 25, 2018. Retrieved July 13, 2018 from https://www.zdnet.com/article/microsoft-heres-why-windows-defender-av-isnt-ranked-higher-in-new-antivirus-tests/.