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 a 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
Table 2. Desirable Windows 10 End-Point Security Tools

<table>
<thead>
<tr>
<th>Isolation</th>
<th>Replication</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyUserName.uwec.edu</td>
<td>Power &amp; sleep settings</td>
<td>Windows defender</td>
</tr>
<tr>
<td>Sign-in options</td>
<td>Backup settings</td>
<td></td>
</tr>
<tr>
<td>Windows defender firewall</td>
<td>Windows update</td>
<td></td>
</tr>
<tr>
<td>Internet security settings</td>
<td>Create a restore point</td>
<td></td>
</tr>
<tr>
<td>User account control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BitLocker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run-as-administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN (GlobalProtect)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Startup applications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:**
  1. Personnel
  2. Intellectual Property
  3. Physical Infrastructure
- **Three Threat Categories:**
  1. 0 Error
  2. 5 Disaster / Accident
  3. Malice
- **Three Mitigation Categories:**
  1. Isolation
  2. Replication
  3. Education

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
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.
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.
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:
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 7. Post Assignment Survey](image)

**Figure 7.** Post Assignment Survey

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.

![Figure 8. Affect Post-Survey at the University of Wisconsin-Eau Claire](image)

**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.

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.
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


