December 2018

An Examination of Cybersecurity Knowledge Transfer: Teaching, Research, and Website Security at U.S. Colleges and Universities

Aditya Gupta
Illinois State University, agupt11@ilstu.edu

James R. Wolf
Illinois State University, jrwolf@ilstu.edu

An Examination of Cybersecurity Knowledge Transfer: Teaching, Research, and Website Security at U.S. Colleges and Universities

Abstract

This work seeks to answer the question: Does faculty cybersecurity knowledge gained from teaching and research transfer to other IT units in the university? Specifically, do colleges and universities that excel in cybersecurity teaching and research have more secure websites? This work explores a unique setting where the knowledge of the source and recipient are both directly related and observable without outside intervention. Our study employed data from 591 U.S. colleges and universities, the National Centers of Academic Excellence (CAE) program, accepted paper data from the ACM Conference on Computer and Communications Security (CCS) and the IEEE Symposium on Security and Privacy (SSP), as well as the results from the SSL Labs Server Test. Our data suggest that universities with cybersecurity research excellence receive higher grades for website security. However, university website security is not significantly associated with cybersecurity teaching excellence, institution size or tuition costs.

INTRODUCTION

The 2016 U.S. Presidential election brought heightened attention to the importance of cybersecurity and the dangers of cybercrime. However, while the public may be just awakening to the seriousness of the issue, the problem has been growing for years. As early as 2012, nearly one in five Americans was the victim of an internet crime (NCSA, 2012). In 2016, the average firm was victimized by two successful cyber-attacks per week (Ponemon Institute, 2016). Cyber-attacks cost the average U.S. firm more than $17 million per year.

The threat of cybercrime is fueling the growing demand for technical and managerial professionals capable of defending public and private networks and safeguarding organizational infrastructure. As the demand for cybersecurity professionals has grown, several colleges and universities have started offering cybersecurity-related degrees. These programs train cybersecurity specialists for both the public and private sectors. They also boost student enrollments and help students land high-paying jobs. Cybersecurity professionals report an average salary of $116,000 (NICCS, 2017).

However, to date, no one has investigated the impact of increased faculty attention to cybersecurity on other IT units within the university. Does cybersecurity knowledge gained from teaching and research transfer to other IT units in the university? Specifically, do colleges and universities that excel in cybersecurity teaching and research have more secure websites?

Extant knowledge transfer research has often relied on self-reported or indirect evidence. This study is unique in that the cybersecurity knowledge of the source unit (i.e., the faculty) and the performance of the recipient unit (i.e., the IT department) are both publicly observable. University faculty demonstrate their cybersecurity knowledge through teaching and research publications. University IT staff demonstrate their cybersecurity knowledge through the configuration of the university's web servers.

The goal of this work is to examine the relationship between faculty cybersecurity teaching and research and the observable security of the university's website. To study our research problem, we will examine data on cybersecurity teaching and research coupled with institutional characteristics and assessments of university web server configurations.

LITERATURE REVIEW

Organizational knowledge transfer is the process of moving pieces of knowledge from one unit (i.e., the source unit) to another (i.e., the recipient unit) (Easterby-Smith, Lyles & Tsang, 2008). According to Smith (2001), explicit knowledge or "know-what" is knowledge that "can be described in formal language, print or electronic media." Tacit knowledge or "know-how" is based on practice and acquired by personal experience (Smith, 2001). Explicit knowledge can be transferred via books, articles or blog posts. Tacit knowledge is more "sticky" or difficult to transfer (Szulanski, 2000). Personal interaction between the knowledge source and recipient is needed to facilitate the transfer of tacit knowledge (Ko et al., 2005).

Knowledge transfer changes the performance of recipient units (Argote & Ingram 2000). As a result, knowledge transfer can be observed by measuring recipient unit performance. Tacit knowledge transfer is enhanced by cognitive proximity or shared knowledge (Forman & van Zeebroeck, 2015). Shared knowledge helps partners better understand the technical knowledge of others. Similarly, organizational proximity, cultural and structural closeness, all promote knowledge transfer by reducing uncertainty and increasing the effectiveness of coordination (Forman & van Zeebroeck, 2015; Levin & Cross, 2004).

Knowledge transfer is associated with physical, cognitive and organizational proximity (Forman & van Zeebroeck, 2015). Physical closeness facilitates social interaction, which is crucial to tacit knowledge transfer (Zucker, Darby & Armstrong, 1998; Zucker, Darby & Brewer, 1998). As a result, knowledge diffuses locally within organizations. For example, the effect of a good teacher spills over to other teachers in the same school (Koedel, 2009). University teaching and research also have spillover effects throughout the region. Firms tend to co-locate in technology clusters near universities to take advantage of these spillover effects (Van Wijk, Jansen & Lyles, 2008). The growth of Silicon Valley and the Boston's Route 128 corridor are often attributed to the teaching and research of local universities (Bania, Eberts & Fogarty, 1993).

Knowledge Transfer Between University IT Faculty and Staff

Living and working in proximity means that there are numerous opportunities for IT faculty and IT staff members to engage in knowledge transfer. On campus, there is a great deal of "cross-pollination" between university information technology faculty and IT staff. University IT staff members, like the staff in all functional areas, often are also alumni of schools where they work. For example, more than 2,400 of Virginia Commonwealth University faculty and staff hold one or more degrees from the university (Working for," 2018). As a result, many of a university's IT staff members will have taken classes from existing IT faculty. Similarly, IT staff often serve with faculty on university committees or teach IT-related courses as adjunct instructors.

Since IT staff and faculty live in the same region, they may volunteer at the same non-profits or belong to the same religious or civic organizations. They may be neighbors, or their kids may attend the same schools or participate in the same activities. These informal connections provide opportunities for the socialization and the exchange of ideas and information. Personal interaction, either face-to-face or electronically, between the knowledge source and recipient facilitates the transfer of tacit knowledge. This exchange of tacit knowledge can be "informal and spontaneous" (Malhotra & Majchrzak, 2012).

Living and working in proximity coupled with the vast amount cross-pollination between IT staff and IT faculty means that there are a large number of potential "boundary spanners." Boundary spanners act as liaisons, facilitating the transfer of information and knowledge between groups (Sonnenwald, 1996). A boundary spanner may be a formal position assigned by the organization, or a role assumed voluntarily (Fleming & Waguespack, 2007). Both direct and indirect interunit relations aid in knowledge transfer by facilitating the search for useful knowledge (Hansen, 2002). These relations help the knowledge seeker learn of "the existence, whereabouts and relevance of substantive knowledge residing in other business units." (Hansen, 2002). In other words, a boundary spanner may not personally possess the needed knowledge, but they know where to find it and can facilitate knowledge transfer by connecting the knowledge seeker to the appropriate person or unit.

Hypotheses

With the growing importance of cybersecurity, there is a strong demand for cybersecurity professionals. This strong demand means that salaries are high for those with cybersecurity skills. Robert Half (2018) reports that the median salary for an Information Systems Security Manager is $137,000. In 2017, there were 350,000 unfilled cybersecurity jobs in the U.S. (Fazzini, 2018). Globally, by 2021, the number of unfilled cybersecurity jobs could grow to 3.5 million (Fazzini, 2018). As a result, colleges and universities need to offer attractive salaries to recruit and retain cybersecurity professionals. Larger organizations have more significant resources and can provide higher compensation (Yanadori & Marler, 2006). Higher compensation may allow larger organizations to better attract and retain IT staff.

In addition, several studies suggest that size has a positive association with knowledge transfer (e.g., Dhanaraj et al., 2004; Gupta & Govindarajan, 2000; Laursen & Salter, 2006). However, there are notable exceptions. Tsang (2002) found no relationship, and Makino and Delios (1996) found a negative association between organizational size and the extent of knowledge transferred. Gupta and Govindarajan (2000) also found that economics played a role in knowledge transfer. Innovative employees require additional compensation. Finally, absorptive capacity, a key facilitator in knowledge acquisition, is positively associated with job satisfaction via compensation (Evans & Davis, 2005). We believe that schools with larger numbers of students will have greater resources to attract and retain high-quality cybersecurity professionals. Further, the bulk of extant research suggests that organizational size has a positive association with knowledge transfer. Thus,

H1. The number of students will be positively associated with university website security.

Schools with larger budgets may be able to offer higher salaries. While tuition is just one of many inputs to a college or university's overall budget, in recent years, tuition's share of the overall budget has been growing. Douglas-Gabriel (2015) reports that in 2003, state funding accounted for 32 percent of state school revenue and tuition contributed 17 percent. By 2012, tuition's portion had grown to 25 percent, and state funding had fallen to 23 percent (Douglas-Gabriel, 2015). As a result, for state schools, tuition is now a more substantial part of the university budget than state funding.

In a study of faculty salaries, Lugt (1983) found that tuition and pay were positively correlated. That is, institutions with higher tuition paid their faculty and staff more than schools with lower tuition. Institutions with higher tuition have larger budgets and can offer more generous compensation packages. This may allow institutions with higher tuition to better recruit and retain high-quality workers—including cybersecurity professionals. Thus,

H2. Tuition costs will be positively associated with university website security.

Source credibility is positively associated with knowledge transfer (for example, Levin & Cross, 2004; Ko, Kirsch, & King, 2005; Slaughter & Kirsch, 2006). Ko et al. (2005) define source credibility as "an attitude a recipient has about a source along multiple dimensions, including trustworthiness and expertise." When source credibility is high, the knowledge receiver is more likely to communicate and collaborate with a knowledge source (Ko et al., 2005). When faculty members have papers accepted at prestigious cybersecurity conferences like the ACM Conference on Computer and Communications Security (CCS) or the Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy (SSP), it not only

demonstrates their excellence in cybersecurity research, it also enhances their source credibility. When a recipient views a source as credible, the recipient is more likely to believe the source is an expert and the knowledge trustworthy (Dholakia and Sternthal, 1977). When a knowledge receiver trusts in the competence of a knowledge source, they are more likely to seek out the source and more likely to learn from the interaction (Levin & Cross, 2004). As a result of increased source credibility, institutions with demonstrated excellence in cybersecurity research should have enhanced cybersecurity knowledge transfer. Thus,

H3. Institutions with cybersecurity research excellence will have more secure university websites.

Colleges and universities designated as DHS/NSA Centers of Academic Excellence in Cybersecurity have completed an in-depth assessment and met rigorous requirements. To receive the designation are evaluated by Subject Matter Experts (SME) with assistance from CAE Program staff ("What is a Center," 2018). These SMEs assess the school's course content, course relevance, laboratory facilities, and faculty involvement, ensuring that faculty have the needed expertise and are providing students the most relevant content ("National Centers of Academic Excellence," 2018).

When a college or university is designated as a DHS/NSA Center of Academic Excellence in Cybersecurity, they not only receive recognition from the federal government, the designation also enhances the source credibility of the school's cybersecurity faculty. In 2017, there were only 177 four-year colleges recognized as NSA/DHS National CAE institutions. As a result of increased source credibility, institutions with demonstrated excellence in cybersecurity teaching should have enhanced cybersecurity knowledge transfer. Thus,

H4. Institutions with cybersecurity teaching excellence will have more secure university websites.
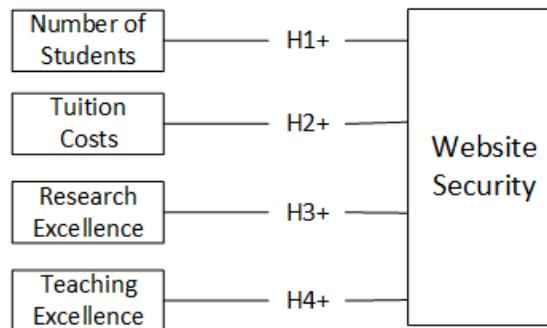

Figure 1: Summary of Hypotheses

DATA GATHERING

For this project, we utilized data from several online sources. Data were extracted, cleaned and analyzed using a combination of Python (van Rossum, 1995) and R scripts (R Core Team, 2017). When available, we used an official or user-created application programming interface (API).

Forbes Top-Rated U.S. Universities List

We started by collecting data on U.S. colleges and universities. Each year, Forbes Magazine posts a list of the top-rated U.S. colleges and universities. The latest installment lists 660 universities (Chuck., 2016). The list includes each university's name, as well as their Forbes ranking, number of students, tuition fees and website Uniform Resource Locator (URL). We accessed the data using R and the *forbesListR* package (Bresler, 2016). The *forbesListR* package facilitates access to the Forbes' list API. The API is useful for obtaining data from the college list and numerous other lists posted by Forbes Magazine.

	Forbes Rank	Students	Tuition
Mean	332.74	11,802.65	$46,971.27
St. Dev.	189.25	12,345.64	$11,879.60
Minimum	1	230	$8,475.00
Maximum	660	81,459	$70,100.00
N	591	591	591

Table 1: Descriptive statistics for all colleges and universities included in study.

National Centers of Academic Excellence

The Department of Homeland Security (DHS) and the National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program. To become an NSA/DHS National CAE designated institution, colleges and universities must meet stringent criteria. CAE institutions receive "formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing the Nation's information systems" (NICCS, 2017).

	Forbes Rank	Students	Tuition
Mean	342.42	23,213.59	$43,431.75
St. Dev.	191.26	13,382.59	$11,686.05
Minimum	3	2,127	$17,718.00
Maximum	659	61,642	$69,912.00
N	112	112	112

Table 2: Descriptive statistics for NSA/DHS National CAE designated institutions.

We were able to obtain the list of CAE institution names and locations using *Web Scrapper* (webscraper.io), a Google Chrome browser extension. Given the stringent criteria needed to earn CAE recognition, we used CAE recognition as a proxy for cybersecurity teaching excellence in our model.

IEEE Symposium on Security and Privacy Data

Next, we gathered information related to cybersecurity research excellence. To this end, we gathered accepted paper data from both the Association for Computing Machinery (ACM) Conference on Computer and Communications Security (CCS) and the Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy (SSP). The conferences are both highly rated with low acceptance rates. From 2007-2016, the ACM CCS had an 18% acceptance rate (Zhou, 2016). Over the same 10-year period, the IEEE SSP had a 13.8% acceptance rate (Zhou, 2016).

For this project, we extracted data from each conference for 2012-2016. Given the high rankings and low acceptance rates, we used paper acceptance at the ACM CCS or IEEE SSP as a proxy for cybersecurity research excellence in our model. To gather IEEE SSP accepted paper data, we used the R statistical programming language and the *IEEER* package (Wiggin & Broman, 2017).

	Forbes Rank	Students	Tuition
Mean	201.71	27,559.94	$52,182.40
St. Dev.	205.42	13,882.08	$12,952.24
Minimum	3	6,298	$27,284.00
Maximum	654	50,320	$69,084.00
N	35	35	35

Table 3: Descriptive statistics for IEEE SSP institutions (2012-2016).

The *IEEER* package is a user-created R interface to the IEEE Xplore Search Gateway. For each IEEE SSP accepted paper, we obtained author names and their university affiliations.

ACM Conference on Computer and Communications Security Data

We extracted accepted paper data from the from the last five (2012-2016) ACM Conferences on Computer and Communications Security (CCS). Unlike the IEEE, the ACM does not have an API that allows easy access to conference and journal publication data.

	Forbes Rank	Students	Tuition
Mean	178.73	28,314.93	$52,958.67
St. Dev	164.58	12,815.30	$11,842.28
Minimum	1	6125	$31,471.00
Maximum	654	58322	$69,912.00
N	60	60	60

Table 4: Descriptive statistics for ACM CCS institutions (2012-2016).

We used Python and the *Beautiful Soup* (Richardson, 2015), *lxml* (Behnel, Faassen, et al., 2017) *pandas* (McKinney, 2010) and *numpy* (van der Walt, Colbert & Varoquaux, 2011) libraries to scrape each year's conference website. For each ACM CCS accepted paper, we obtained author names and university affiliations.

	ACM	IEEE
Mean	0.90	0.29
Std Dev	4.69	1.75
Maximum	61	23
Minimum	0	0
Schools with publications	60	35
Schools without publications	531	556

Table 5: Papers accepted at ACM CCS and IEEE SSP by school (2012-2016).

In Table 5, *ACM* schools are institutions with faculty who have had papers accepted at the ACM Conference on Computer and Communications Security (CCS). Similarly, *IEEE* schools are institutions with faculty who have had papers accepted at the IEEE Symposium on Security and Privacy (SSP).

In our data, only a small number of schools (n = 62) had faculties with the research proficiency needed to publish their work at IEEE SSP or ACM CCS. In the past five years, only 24 institutions had faculty publish their work at both IEEE SSP and ACM CCS.

SSL Labs Grades for University Websites

The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), use encryption to protect data communicated between browsers and web applications (Dierks, 2008; & Freier, Karlton & Kocher, 2011). The two protocols, commonly referred to as SSL/TLS or simply SSL, are the de facto Internet standards for safeguarding the privacy of Internet data (Church, Moloney & Bannister, 2013).

The SSL Labs Server Test is a free online tool to assess SSL\TSL server configurations. The test examines a certificate to verify that it is valid and trusted (Ristić, 2017). It also examines server configuration for protocol support, key exchange support, and cipher support. The test also examines a certificate to verify that it is valid and trusted. After examining these four areas, the area scores combined into an overall score and an academic letter grade (*A+, A, A-, B, C* or *F*) is calculated. These letter grades are adjusted downward if the server has not implemented specific patches, or if exploitable vulnerabilities are detected. For example, if the server is deemed

In certain situations, the SSL Labs Server Test will not provide a (*A+ - F*) letter grade. For example, if the site certificate is not trusted the test will issue grade of *T*. If there is a certificate name mismatch, the test will issue grade of *M*. As the SSL Labs Server Test documentation notes, if the site certificate is not trusted or there is a certificate name mismatch, the actual security grade is irrelevant because active network attackers will be able to subvert connection security (Ristić, 2017).

SSL Server Test Grade	Number of Schools
A+	13
A	237
A-	56
B	104
C	89
F	92
Total	591

Table 6: SSL Labs Server Test Grades.

There is one other situation where the SSL Labs Server Test will not produce an (*A+ - F*) letter grade when the organization has asked SSL Labs not to permit tests on its servers. One school in our list requested that their web servers not be tested. In all cases where SSL Labs could not, or would not, provide an (*A+ - F*) letter grade, we dropped the college or university from our analysis.

On July 01, 2017, there were 177 four-year colleges recognized as NSA/DHS National CAE institutions. Of these, 65 either were not on the Forbes list or received a grade of *T* or *M* on the SSL Server Test. We dropped these schools from our analysis. We also dropped military service academies from our analysis. Our resulting dataset contained 591 schools, including 112 colleges or universities recognized as NSA/DHS National CAE institutions.

SSL Server Grade	CAE Schools	ACM Schools	IEEE Schools	All Schools
A+	3	2	0	13
A	43	24	16	237
A-	12	5	5	56
B	23	17	7	104
C	18	6	4	89
F	13	6	3	92
Total	112	60	35	591

Table 7: SSL Labs Server Test Grades by school type.

In Table 7, *CAE Schools* are colleges recognized as NSA/DHS National CAE institutions, *ACM Schools* are institutions with faculty who have had papers accepted at the ACM Conference on Computer and Communications Security (CCS), and *IEEE Schools* are institutions with faculty who papers accepted the IEEE Symposium on Security and Privacy (SSP). *All Schools* includes all 591 colleges and universities in our dataset.

While 20% of all web servers tested received an *F* grade on the SSL Server Test (Qualys Inc., 2018), 92 schools (16%) in our dataset received *F* grades. Just under 12% of CAE schools, 10% of ACM Schools and 9% of IEEE schools received *F* grades. To aid in analysis, we converted the SSL Server Test letter grades to their academic numeric equivalent. We followed the method that is commonly employed in the United States for calculating students' grade point average (GPA) (Stanford University, 2017).

	CAE Schools	Non-CAE Schools	All Schools
Mean	2.99	2.85	2.88
St. Dev.	1.31	1.45	1.42
Minimum	0.00	0.00	0.00
Maximum	4.33	4.33	4.33

Table 8: SSL Labs Server Test result statistics for NSA/DHS National CAE schools.

	IEEE	ACM	Neither	All Schools
Mean	2.86	3.10	3.19	2.88
St. Dev.	1.44	1.23	1.19	1.42
Minimum	0.00	0.00	0.00	0.00
Maximum	4.33	4.33	4.00	4.33

Table 9: SSL Labs Server Test result statistics for IEEE SSP and ACM CCS schools.

In Table 8, *CAE Schools* are colleges recognized as NSA/DHS National CAE institutions and *Non-CAE Schools* denote colleges that are not CAE institutions. In Table 9, *ACM Schools* are institutions with faculty who have had papers accepted at the ACM Conference on Computer and Communications Security (CCS). Similarly, *IEEE Schools* are institutions with faculty who have had papers accepted at the IEEE Symposium on Security and Privacy (SSP). *Neither* schools include institutions without accepted papers at either the CCS or SSP. In both Tables 8 and 9, *All Schools* includes all 591 colleges and universities in our dataset.

RESULTS AND OUTCOMES

As the response variable, *SSL Server Test Grade* is ordinal, we first attempted to use ordered logistic regression analysis. One of the fundamental assumptions of ordinal logistic regression is that the relationship between each pair of outcome groups is the same (UCLA: Statistical Consulting Group, 2016; Williams, 2016). This is called the proportional odds (PO) assumption (or the parallel-lines assumption) (Harrell, 2013).

The omnibus Brant Test (Brant, 1990), suggested that the PO assumption for the model was violated. Examining each predictor, we found that two predictor variables, *Research* and *Teaching*, met the assumption, while the assumption did not hold for *Tuition Costs* and *Number of Students*. The Brant Test was significant for both *Tuition Costs* (χ^2 (4) = 13.48, p = .009) and *Number of Students* (χ^2 (4) = 19.13, p = .001). For this reason, a partial propositional odds (PPO) model was chosen. The PPO model allows the effects of predictor variables to vary when the proportional odds assumption does not hold (Liu, 2015).

We used Stata 14 (StataCorp, 2015) and the *gologit2* package (Williams, 2006) to estimate the ordinal outcome variable *SSL Server Test Grade*. The predictor variables were *Tuition Costs*, *Number of Students*, Cybersecurity Research Excellence (*Research*) and Cybersecurity Teaching Excellence (*Teaching*).

VARIABLES	(All) SSL Grade	(1) F vs C,B, A-, A , A+	(2) F , C vs B, A-, A, A+	(3) F , C, B vs A-, A, A+	(4) F , C, B , A- vs A, A+	(5) F , C, B , A- vs A+
Teaching Excellence	-0.0964					
	(0.219)					
Research Excellence	0.592**					
	(0.300)					
Tuition Costs		0.204	0.0589	-0.510	-0.753**	-3.284***
		(0.500)	(0.402)	(0.369)	(0.370)	(1.199)
Number of Students		0.396***	0.168	-0.0689	-0.179*	-0.682*
		(0.151)	(0.111)	(0.101)	(0.102)	(0.389)
Constant		1.719***	0.789***	0.0324	-0.352***	-4.166***
		(0.129)	(0.100)	(0.0939)	(0.0951)	(0.366)
Observations	591					
Pseudo R-Squared	0.0179					
ll	-902.0					
df_m	12					
chi2	32.92					

Standard errors in parentheses
*** *p<0.01, ** p<0.05, * p<0.1*

Table 10: Results of the Partial Proportional Odds Model using gologit2—Coefficients.

Table 10 presents the coefficients and standard errors of the predictor variables. The log likelihood ratio chi-square statistic LR χ^2 (12) = 32.92, p < .001, indicated that the model was significant. Two predictor variables *Research* and *Teaching*, those meeting the PO assumption, had the same regression coefficients across all binary models. For *Research*, β = .592, p = .048; and for *Teaching*, β = -.096, p = .660.

VARIABLES	(All) SSL Grade Log Odds	(1) F vs C,B, A-, A , A+	(2) F , C vs B, A-, A, A+	(3) F , C, B vs A-, A, A+	(4) F , C, B , A- vs A, A+	(5) F , C, B , A- vs A+
Teaching Excellence	0.908					
	(0.199)					
Research Excellence	1.807**					
	(0.541)					
Tuition Costs		1.226	1.061	0.600	0.471**	0.0375***
		(0.613)	(0.426)	(0.222)	(0.174)	(0.0450)
Number of Students		1.485***	1.183	0.933	0.836*	0.506*
		(0.225)	(0.131)	(0.0942)	(0.0855)	(0.197)
Constant		5.577***	2.202***	1.033	0.703***	0.0155***
		(0.718)	(0.221)	(0.0970)	(0.0669)	(0.00568)
Observations	591					
Pseudo R-Squared	0.0179					
ll	-902.0					
df_m	12					
chi2	32.92					

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 11: Results of the Partial Proportional Odds Model using gologit2—Odds Ratios.

Table 11 presents the odds ratios and standard errors of the predictor variables. For the *Research* predictor, OR = 1.807, p =.048, which indicates that the odds of receiving a higher *SSL Grade* were 80.7% higher than the odds for a school without research when adjusting for other predictors (Williams, 2006; Liu, 2015). For the *Teaching* predictor, OR = .908, p =.660, which indicates that there was not a significant relationship between *Teaching* and the cumulative odds of earning a higher *SSL Grade*.

The odds ratios for *Tuition Costs* were different across each binary model. The ratios were 1.226, 1.061, .600, .471 and .037 respectively. The odds were decreasing across cut lines. Only the 4th (p = .042) and 5th models (p = .006) appear significant. The odds ratios for *Number of Students* were different across each binary model. The ratios were .412, .184, -.057, -.169 and -.6716 respectively. The odds were decreasing across cut lines. Only model 1 (p = .009) appears significant.

As the response variable, *SSL Server Test Grade* is ordinal, we first attempted to use ordered logistic regression analysis. One of the fundamental assumptions of ordinal logistic regression is that the relationship between each pair of outcome groups is the same (UCLA: Statistical Consulting Group, 2016; Williams, 2016). This is called the proportional odds (PO) assumption (or the parallel-lines assumption) (Harrell, 2013).

The omnibus Brant Test (Brant, 1990), suggested that the PO assumption for the model was violated. Examining each predictor, we found that two predictor variables, *Research* and *Teaching*, met the assumption, while the assumption did not hold for *Tuition Costs* and *Number of Students*. The Brant Test was significant for both *Tuition Costs* (χ^2 (4) = 13.48, p = .009) and *Number of Students* (χ^2 (4) = 19.13, p = .001). For this reason, a partial propositional odds (PPO) model was chosen. The PPO model allows the effects of predictor variables to vary when the proportional odds assumption does not hold (Liu, 2015).

DISCUSSION

Our analysis suggests that there is a positive and significant association between a college or university's website cybersecurity and faculty with cybersecurity research excellence. Thus, Hypothesis 3 is supported. However, our data suggest that there is a negative, but not statistically significant association between a college or university's website cybersecurity and tuition costs. Thus, Hypothesis 1 is not supported. Similarly, our analysis does not support Hypothesis 2. Our data suggest that there is a negative, but not statistically significant, association between a college or university's website cybersecurity and the size of the student body. Finally, Hypothesis 4 is also not supported. Our data suggest that there is a negative, but not significant association between the security of the college or university's website and cybersecurity teaching excellence.

CONCLUSION

While there is a rich history of IT research examining the role of information technology in knowledge transfer (for example, Alavi and Leidner 2001; Markus, 2001; & Malhotra et al., 2005) and examining knowledge transfer in software development (for example, Ko et al., 2005; Pavlou & El Sawy, 2006; & Joshi et al., 2007), this work the first to investigate cybersecurity knowledge sharing between academic faculty and IT staff. This work contributes to both the literature on cybersecurity and knowledge transfer.

The bulk of knowledge transfer research employs self-reported or indirect evidence. In most settings, it is difficult to determine which organizations possess superior, or inferior, technical skills and to separate marketing hype from actual prowess. It can also be difficult to obtain objective measures of an organization's true technical skills (Grant & Verona, 2015). However, universities are unique organizations in that their workers (faculty) publicize their expertise (teaching and research). This makes it easier to measure their expertise in cybersecurity. This study is unique in that the knowledge flow at both ends is fully observable. The source unit (i.e., the faculty) and the recipient unit (i.e., the IT department) both publicly display their cybersecurity knowledge. In addition, the SSL Labs Server Test (Qualys Inc., 2016) gives us a significant, and publicly available, measure of each university's website security.

Our findings suggest that college and universities with research excellence, regardless of size or tuition costs, have more secure websites. More work is needed to determine why research excellence was associated with higher SSL grades, but teaching excellence was not.

Several researchers have noted that knowledge transfer between units is not easy or typical. Von Hippel (1994) used the term 'stickiness' to describe this difficulty. Szulanski (2006) suggested that characteristics of the source of knowledge, characteristics of the recipient of knowledge, and characteristics of the context contribute to the stickiness of knowledge. Szulanski (2000) found that the recipient perceptions of the reliability of the source were associated with the difficulty of knowledge transfer. Our findings may suggest that university IT staff may attach more weight to ACM CCS or IEEE SSP publications than the NSA/DHS National CAE designation.

	CAE Schools	ACM Schools	IEEE Schools	IEEE or ACM	Both IEEE and ACM
Mean	342.42	178.73	201.71	180.47	131.75
St. Dev.	191.26	164.58	205.42	176.94	141.92
Minimum	3	1	3	1	3
Maximum	659	654	654	654	654
N	112	60	35	62	24

Table 12: Forbes Rankings for NSA/DHS National CAE, IEEE and ACM schools.

As Table 12 shows, IEEE and ACM institutions have higher Forbes Rankings. NSA/DHS National CAE designated institutions have lower average rankings than schools that are not CAE designated institutions (i.e., non-CAE institutions) in our sample. As a result, IT staff may not trust the relevance or usefulness of CAE faculty knowledge. However, our data suggest that only a small number of schools have faculty with the research proficiency needed to publish their work at IEEE SSP or ACM CCS.

Another possible explanation is the frequency of the cybersecurity-related events. NSA/DHS National CAE designation is a single event, but research publications potentially occur more frequently. Perhaps the higher frequency makes publication announcements more salient and creates the impression of greater cybersecurity activity.

It may also be the case that colleges and universities that put a premium on research excellence also place more emphasis on knowledge transfer. Worasinchai and Daneshgar (2012) note that transfer capability is a critical factor for the knowledge source, and absorptive capacity is a critical factor for the knowledge recipient.

As cybersecurity grows in significance, it is essential to understand the flow of cybersecurity knowledge within organizations and to identify the factors that aid or inhibit the flow of this knowledge between IT units. The next step in this research is to survey cybersecurity faculty and university IT staff to examine motivation, absorptive capacity, transfer capability, arduous relationship and other factors known to impact organizational knowledge transfer.

REFERENCES

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues, *MIS Quarterly* 25(1), 107-136.

Bania, N., Eberts, R. W., & Fogarty, M. S. (1993). Universities and the startup of new companies: can we generalize from Route 128 and Silicon Valley? *The Review of Economics and Statistics*, 75, 761-766

Brant, R. (1990). Assessing proportionality in the proportional odds model for ordinal logistic regression. Biometrics, 1171-1178.Behnel, S. Faassen, M., et al. (2017). http://lxml.de Accessed 05 July 2017

Bresler, Alex. (2016). R Wrapper for the Forbes List API. https://github.com/abresler/forbesListR Accessed on July 11, 2017

Chuck, Elizabeth. (2016). These are the top colleges of 2016, According to Forbes. Retrieved from http://www.nbcnews.com/feature/college-game-plan/these-are-top-colleges-2016-according-forbes-n605391

Church, L., Moloney, M., & Bannister, F. (2013, January). The Sealed Letter: Safeguarding the Public System of Privacy Protection in a Digital World. In System Sciences (HICSS), 2013 46th Hawaii International Conference on (pp. 1973-1982).

Dhanaraj, C., Lyles, M. A., Steensma, H. K., & Tihanyi, L. (2004). Managing tacit and explicit knowledge transfer in IJVs: the role of relational embeddedness and the impact on performance. *Journal of International Business Studies*, *35*(5), 428-442.

Dholakia, R., & Sternthal, B. (1977). Highly credible sources: Persuasive facilitators or persuasive liabilities?. *Journal of Consumer Research*, *3*(4), 223-232.

Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version 1.2 (No. RFC 5246).

Douglas-Gabriel, D. (2015, January 5). Students now pay more of their public university tuition than state governments. The Washington Post. Retrieved from https://www.washingtonpost.com/news/get-there/wp/2015/01/05/students-cover-more-of-their-public-university-tuition-now-than-state-governments/

Easterby-Smith, M., Lyles, M. A., & Tsang, E. W. (2008). Inter-organizational knowledge transfer: Current themes and future prospects. *Journal of Management Studies*, *45*(4), 677-690.

Evans, W. R., & Davis, W. D. (2005). High-performance work systems and organizational performance: The mediating role of internal social structure. *Journal of Management*, 31(5), 758-775.

Fazzini, K. (2018). You don't need to be a hacker to get a high-paying cybersecurity job. CNBC . Available at: https://www.cnbc.com/2018/08/09/cybersecurity-jobs-non-technical-workers.html. (Accessed: 01 August 2018)

Fleming, L., & Waguespack, D. M. (2007). Brokerage, boundary spanning, and leadership in open innovation communities. *Organization Science*, 18(2), 165-180.

Forman, C. M., & van Zeebroeck, N. (2015, January). Internet adoption and knowledge diffusion. In Academy of Management Proceedings (Vol. 2015, No. 1, p. 14164). Academy of Management.

Freier, A., Karlton, P., & Kocher, P. (2011). The secure sockets layer (SSL) protocol version 3.0.

Grant, R. M., & Verona, G. (2015). What's holding back empirical research into organizational capabilities? Remedies for common problems. *Strategic Organization*, 13(1), 61-74.

Gupta, A. K., & Govindarajan, V. (2000). Knowledge flows within multinational corporations. *Strategic Management Journal*, 21(4), 473-496.

Hansen, M. T. (2002). Knowledge networks: Explaining effective knowledge sharing in multiunit companies. *Organization Science*, 13(3), 232-248.

Harrell, F. E. (2013). *Regression modeling strategies: with applications to linear models, logistic regression, and survival analysis*. Springer Science & Business Media.

IEEE Security & Privacy, Aim & Scope. Retrieved from http://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=8013

Joshi, K. D., Sarker, S., & Sarker, S. (2007). Knowledge transfer within information systems development teams: Examining the role of knowledge source attributes. *Decision Support Systems*, 43(2), 322-335.

Ko, K., Kirsch, L., & King, W. (2005). "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations", *MIS Quarterly*, Vol. 29(1), pp. 59-85.

Koedel, C. (2009). An empirical analysis of teacher spillover effects in secondary school. *Economics of Education Review*, *28*(6), 682-692.

Laursen, K., & Salter, A. (2006). Open for innovation: the role of openness in explaining innovation performance among UK manufacturing firms. *Strategic Management Journal*, *27*(2), 131-150.

Levin, D. Z., & Cross, R. (2004). The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer. *Management Science*, 50(11), 1477-1490.

Levina, N., & Vaast, E. (2005). The emergence of boundary spanning competence in practice: implications for implementation and use of information systems. *MIS Quarterly*, 335-363.

Liu, X. (2015). *Applied Ordinal Logistic Regression Using Stata: From Single-level to Multilevel Modeling*. Sage Publications.

Lugt, K. V. (1983). Correlations Between Faculty Salaries and Tuition at Private Undergraduate Colleges: Who's Underpaid?. *The Journal of Higher Education*, 54(4), 399-406.

Makino, S., & Delios, A. (1996). Local knowledge transfer and performance: Implications for alliance formation in Asia. *Journal of International Business Studies*, *27*(5), 905-927.

Malhotra, A., Gosain, S., & El Sawy, O. A. (2005). Absorptive Capacity Configurations in Supply Chains: Gearing for Partner Enabled Market Knowledge Creation, *MIS Quarterly* (29:1), pp. 145-187.

Malhotra, A., & Majchrzak, A. (2012). How virtual teams use their virtual workspace to coordinate knowledge. *ACM Transactions on Management Information Systems (TMIS)*, 3(1), 6:1-6:14.

Markus, M. L. (2001). Toward a Theory of Knowledge Reuse: Types of Knowledge Reuse Situations and Factors in Reuse Success, *Journal of Management Information Systems* (18:1), pp. 57-93.

McKinney, W. (2010). Data structures for statistical computing in python. In *Proceedings of the 9th Python in Science Conference* 445, 51-56.

National Centers of Academic Excellence in Cyber Defense (CAE-CD) Program Guidance. (2018). Available at: https://niccs.us-cert.gov/sites/default/files/documents/pdf/cae_program_guidance.pdf?trackDocs=cae_program_guidance.pdf.

National Cyber Security Alliance (NCSA), "2012 NCSA / McAfee Online Safety Survey," National Cyber Security Alliance, Oct. 2012. Available at: https://staysafeonline.org/wp-content/uploads/2017/09/2012-NCSA-McAfee-Online-Safety-Study.pdf Accessed 05 July 2017

National Initiative for Cybersecurity Careers and Studies (NICCS). (2017). National Centers of Academic Excellence (CAE). https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae Accessed July 07 2017

Pavlou, P. A., & El Sawy, O. A. (2006). From IT Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development, *Information Systems Research* (17:3), pp. 198-227.

Ponemon Institute. (2016) 2016 Cost of Cyber Crime Study & the Risk of Business Innovation. Available from: http://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation Accessed 05 July 2017

Qualys, Inc. (2017) SSL Labs APIs https://www.ssllabs.com/projects/ssllabs-apis/ Accessed 05 July 2017

R Core Team (2017). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL https://www.R-project.org/.

Richardson, L. (2015). Beautiful Soup Documentation. Accessed 05 July 2017 https://www.crummy.com/software/BeautifulSoup/bs4/doc/

Ristić, I. (2017). About SSL Labs. Retrieved from https://www.ssllabs.com. Accessed July 12 2017.

Ristić, I. (2017) SSL Server Rating Guide https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide. Accessed July 12 2017.

Robert Half. (2018). Robert Half 2018 Salary Guide for Technology professionals. Available at: https://www.roberthalf.com/sites/default/files/documents/2018_salary_guide_NA_technology_1.pdf. (Accessed: 01 August 2018).

Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, 5(4), 311-321.

Qualys Inc. SSL Labs. (2016). SSL Pulse. From https://www.ssllabs.com/ssl-pulse/ (accessed January 23, 2016).

Qualys Inc. SSL Labs. (2018). SSL Server Rating Guide. Qualys Inc. SSL Labs. From https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide/ (accessed August 01, 2018).

StataCorp. 2015. Stata Statistical Software: Release 14. College Station, TX: StataCorp LP.

Slaughter, S. A., & Kirsch, L. J. (2006). The effectiveness of knowledge transfer portfolios in software process improvement: A field study. *Information Systems Research*, *17*(3), 301-320.

Sonnenwald, D. H. (1996). Communication roles that support collaboration during the design process. *Design Studies*, 17(3), 277-301.

Stanford University. (2017). How the General University GPA is Determined. https://registrar.stanford.edu/students/definition-grades/grade-point-average-gpa-and-class-rank-policy/how-general-university-gpa Accessed July 01, 2017.

Szulanski, G. (2000). The process of knowledge transfer: A diachronic analysis of stickiness. *Organizational Behavior and Human Decision Processes*, *82*(1), 9-27.

Szulanski, G., & Jensen, R. J. (2006). Presumptive adaptation and the effectiveness of knowledge transfer. *Strategic Management Journal*, *27*(10), 937-957.

Tsang, E. W. (2002). Acquiring knowledge by foreign partners from international joint ventures in a transition economy: learning-by-doing and learning myopia. *Strategic Management Journal*, *23*(9), 835-854.

Tushman, M. L. (1977). Special boundary roles in the innovation process. *Administrative Science Quarterly*, 587-605.

UCLA: Statistical Consulting Group. (2011). R Data Analysis Examples: Ordinal Logistic Regression. http://www.ats.ucla.edu/stat/r/dae/ologit.htm/ (accessed January 06, 2016).

Van der Walt, S. Colbert, C., & Varoquaux, G. (2011). The NumPy Array: A Structure for Efficient Numerical Computation, *Computing in Science & Engineering*, 13, 22-30. DOI:10.1109/MCSE.2011.37

Van Rossum, G. (1995). Python tutorial, Technical Report CS-R9526, Centrum voor Wiskunde en Informatica (CWI), Amsterdam.

Van Wijk, R., Jansen, J. J., & Lyles, M. A. (2008). Inter-and intra-organizational knowledge transfer: a meta-analytic review and assessment of its antecedents and consequences. *Journal of Management Studies*, 45(4), 830-853

Von Hippel, E. (1994). "Sticky information" and the locus of problem solving: implications for innovation. *Management Science*, *40*(4), 429-439.

Wiggin, S., & Broman, K. (2017). IEEER: Interface to the IEEE Xplore Gateway. R package version 0.2.9. Accessed 05 July 2017

Williams, R. (2016). Understanding and interpreting generalized ordered logit models. *The Journal of Mathematical Sociology*, *40*(1), 7-20.

Williams, R. (2006). Generalized ordered logit/partial proportional odds models for ordinal dependent variables. *Stata Journal*, 6(1), 58-82.

What is a Center of Academic Excellence (CAE)? (2018). Available at: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/. (Accessed: 01 August 2018)

Worasinchai, L., & Daneshgar, F. (2012). A qualitative analysis of knowledge transfer in global supply chains: Case of Thai distributer of imported products. *Electronic Journal of Knowledge Management*, 10(2), 195-204.

Working for alma mater. (2018, April 14). Retrieved from: https://news.vcu.edu/article/Working_for_alma_mater.

Yao, F. K., & Chang, S. (2017). Do individual employees' learning goal orientation and civic virtue matter? A micro-foundations perspective on firm absorptive capacity. *Strategic Management Journal*, 38(10), 2041-2060.

Yanadori, Y., & Marler, J. (2006). Compensation strategy: does business strategy influence compensation in high-technology firms?. *Strategic Management Journal*, *27*(6), 559-570.

Zhou, J. (2016). Top Cyber Security Conferences Ranking http://jianying.space/conference-ranking.html, Accessed 05 July 2017

Zucker, L., Darby, M., & Brewer, M. (1998). Intellectual Capital and the Birth of U.S. Biotechnology Enterprises, *American Economic Review*, 88, 290-306.

Zucker, L., Darby, M., & Armstrong, J. (1998). Intellectual Capital and the Firm: The Technology of Geographically Localized Knowledge Spillovers, *Economic Inquiry*, 36, pp. 65-86.