Journal of Information Technology Education: Discussion Cases

10/17/2017

UTKARSH SHRIVASTAVA, TAUFEEQ MOHAMMED

A CYBERSECURITY EXECUTIVE DBA?[1]

Risk doesn't scare me. What scares me is rushing into things without thinking through.
—Moez Limayem, Dean, Muma College of Business, University of South Florida

Grandon Gill, Academic Director of the Doctorate of Business Administration Program (DBA) at the University of South Florida's (USF) Muma College of Business pondered the email he had just sent to Moez Limayem, the dean of the college (see Exhibit 1). In that email, he had raised the possibility of developing a version of the college's highly successful DBA program specifically targeting cybersecurity professionals. He also noted the possibility of funding from the National Science Foundation (NSF) to help cover the costs of launching the program.

The idea of starting the program sparked when Gill had attended an NSF principal investigator's meeting earlier in the year. A key area of discussion in the meeting involved the serious shortage of terminally qualified faculty candidates to teach cybersecurity-related graduate courses at universities across the United States. These discussions were confirmed by subsequent research. Recent surveys by the U.S. Department of Labor found that the demand for cybersecurity graduates had increased by 27% in 2016 to reach a record high, and increasing number of data breaches and cyber-attacks highlighted the need for trained security professionals. Although there was a lot of practical experience out there in the cybersecurity arena, when a research university like USF wanted to hire faculty, candidates needed to have a terminal degree such as a PhD or DBA. These were much less common among the security experts that would be a good fit with business schools or MIS departments. Indeed, there were few doctoral programs in cybersecurity that focused on researching the human side of cybersecurity—increasingly important in the worlds of business and government. The Muma College of Business has experienced many challenges in its own efforts to hire cybersecurity faculty. What Gill also recognized was that much of the research content of the DBA program that he led could be quite applicable to nontechnical cybersecurity research.

The possibility of initiating the new program was not a decision to be taken lightly. Indeed, it raised a series of related questions and decisions: 1) Would such a program be viable in the first place? 2) Should the launch of such a program be contingent on the acquisition of external funding to cover startup expenses? 3) Could the DBA program faculty and staff, already stretched thin by the DBA program's larger than expected cohorts, support such an additional program? 4) At a university where responsibility for cybersecurity was spread across three colleges, what type of support or opposition could be anticipated for such a program?

Developing Cybersecurity Professionals

A complex system of wired and wireless networks connected individuals and organizations across the world. As the world order became increasingly dependent on the exchange of information through these networks, ensuring the security of these networks—keeping access to these networks available, while maintaining the privacy of data contained within them and protecting from unauthorized destruction or modification—was becoming a top priority. Unfortunately, the goal of accessibility tended to conflict with that of protecting data. Thus, cyber-attacks had become so contagious that the saying "One bad fish can spoil the whole pond." fitted well in the context of computer networks. A record 79% of the U.S. businesses reported a cybersecurity incident in the year 2016, and the reporting organization believed that it was the best-case scenario as they expected that many of these incidents were either not detected or not reported (Raytheon, 2015).

Demand for Professionals

With an increase in the cybersecurity related incidents, the demand for professionals with expertise in monitoring and securing IT infrastructure was also going up. Businesses had started taking the information security concerns more seriously, and it was expected that the cybersecurity market would grow from $75 billion in 2015 to $170 billion by 2020 (Morgan, 2015). A career in cybersecurity demanded creativity as well as analytical and technical prowess, but it offered diverse options for the aspirants. The cybersecurity career track included designations such as Cyber Behavior Scientist (to study human behavior), Vulnerability Researcher (to identify pitfalls and weaknesses in software) and Information Assurance Engineer (to protect hardware from cyber-attacks). The Department of Homeland Security listed at least 31 common areas within the cybersecurity profession that prospective job candidates could choose from (NICCS, 2017).

According to the leading security firm Symantec, there would be a shortfall of 1.5 million cybersecurity professionals by 2019 against the total global demand of 6 million (see Exhibit 2). To address the expected shortfalls, universities needed to add cybersecurity programs. A serious constraint that limited the development of such programs was the shortage of qualified faculty, particularly research faculty. In a 2013 report, the National Academies of Science characterized cybersecurity as an emerging discipline. As with most of the emerging fields, there were few graduate programs in the area, and the curriculum was not coherent amongst them. This resulted in different departments (such as engineering, business or law) in the same university offering their own versions of cybersecurity education. Gradually, academics were coming to the realization that cybersecurity was an intrinsically interdisciplinary area. Focusing only on the technical aspects related to cybercrime would hinder the development of useful solutions. The ideal researcher would be able to draw upon multiple perspectives, both technical and behavioral.

Existing Educational Structures

The first step in the direction of formalizing the education given to cybersecurity students in the colleges was taken by the National Security Agency (NSA). The National Center of Academic Excellence in Cyber Defense (NCAECD) program was started in 1998 to produce graduates that met the specific needs (mostly related to coding ability) of the agency. This move by the federal agency encouraged many colleges to focus on the technical aspects of cybersecurity. By 2016, about 200 colleges had earned the designation given by NCAECD which ensured the students and the employers that the cybersecurity education followed the standards set by NSA (NSA, 2016). In addition, the Department of Education and NSF were also partnering to develop cybersecurity programs based on science, technology, engineering and math (STEM) disciplines to address the shortage of the skilled workforce. The acute shortage of workforce meant that even the graduates with non-STEM focused degrees could get entry level jobs after getting the requisite training from the hiring firms.

Early cybersecurity programs focused mainly on the technical coding skills as they were required by the NSA and were also a key component of the curriculum developed under NCAECD. The cybercriminals, however, kept on defying odds and developed creative ways of getting access to the vulnerable systems. Their success was attributed to variability, and delay in adoption of updated systems and protocols at the global level. The computer networks or internet functioned as an integrated system, and an outdated node or protocol in the network could become an opening for a contagious cyber-attack. One of the reasons for hackers having the upper hand was their ability to identify weak links and avenues for cyber-attacks from computers and humans operating them. They had the knack of getting their job done even in the presence of a secure hardware/software apparatus in place. It was becoming clearer that human behavior played a key role in cybercrimes and was something which could not be modeled using mathematical algorithms or by learning coding skills.

Emerging Needs

The researchers in the cybersecurity area suggested the need for training a new breed of professionals who could understand the human and legal aspects of the cybercrimes (Shoemaker & Kohnke, 2016). The need of the hour was to determine the avenues for a cyberattack before the hackers did and take appropriate actions to prevent it. On the other hand, if such an attack took place, then a cybersecurity expert should understand the criminal law and computer forensics to be able to track and find evidence, and prosecute the attacker. Paralleling what researchers were recognizing, educational institutions began to construct cybersecurity programs as interdisciplinary concentrations that required students to learn a variety of topics before graduation. To achieve this, the faculties had started adding cybersecurity electives or concentrations in engineering, management, and psychology degrees as well. The U.S. Naval Academy started teaching technical skills in the early years of its undergraduate program, then applying these learned skills to policy, law, and other fields in the later years of the program. Northeastern University branded their cybersecurity graduates as “cyberliaisons” for their expertise in computers and policy related issues while Le Moyne College in Syracuse marketed their cybersecurity program as “cybersecurity for presidents” aimed at producing corporate leaders.

Cybersecurity Doctoral Programs

Cybersecurity programs were seeing a massing jump in the number of enrollments. For instance, the enrollment to Dakota State University (DSU) cybersecurity program rose by more than 200% within a span of five years while it increased by more than 300% at Harvard University within two years (Raposa, 2017). Apart from job security, top tier institutions such as Harvard and Indiana University customized their cybersecurity curriculums to meet the requirements of marketing executives, lawyers, managers, and so forth. Even community colleges were witnessing an increase in enrollment in their cybersecurity certificate programs--benefiting from lower costs, flexible academic requirements, and attractive employment opportunities. Program development support was offered through security technology centers and through projects sponsored by the NSF. The result: a surge in the number of cybersecurity programs with around 200 new Centers for Excellence in Cybersecurity within a span of 9 years.

The sudden rise in the number of enrollments and new cybersecurity graduate programs was in turn leading to a shortage of terminally qualified faculty candidates for the teaching positions. Institutions such as University of Connecticut and University of South Florida were advertising dozens of faculty positions in the cybersecurity area. There was no shortage of candidates with applied field experience in combating cybercrimes. Those holding terminal degrees in the area were scarce, however. With more than 200 schools offering cybersecurity credentials ranging from certificates, associate’s, bachelor’s and master’s degrees--the doctoral degree appeared to be the next logical step (Collins, Soo Hoo, Krantz, & Cosgrove, 2012).

Most of the doctoral degrees with a cybersecurity concentration were offered by the computer engineering departments across the United States. The students enrolled into these programs had the option to typically choose amongst the two focus areas of "information security" and "information assurance." A computer science PhD degree with "information security" focus generally emphasized concepts related to computational practice such as algorithms, network architecture, and artificial intelligence. A PhD in computer science with an "information assurance" focus area emphasized the impact of cyber laws, policy, and human behavior on the security preparedness. Typically, a computer science undergraduate degree was an essential requirement for getting admission to these programs, and full-time residency was also a frequent requirement. An example of the structure of a typical program, offered by Arizona State University, is presented in Exhibit 3.

Some institutions such as Purdue University offered interdisciplinary PhD programs in information security. These programs were essentially started for the students who had a different set of skills and background, or had done research in topics that were difficult to support in the existing disciplines. Cybersecurity being an emerging field and known for its multidisciplinary focus was expected to attract students in such interdisciplinary programs. At Purdue, the program was sponsored by the departments of communication and philosophy, college of technology and program linguistics. These departments had an option to specify their own requirements for the program students. Interestingly, though computational background was preferred, the admission committee was flexible regarding the undergraduate major.

External funding sources, such as NSF, provided financial support to studies that bridged gaps across the disciplines. Iowa University responded to the needs of the students and the priorities of the funding agencies by bringing together the faculties of different departments, such as engineering, mathematics, and political science within its Information Assurance Center (IAC). IAC offered graduate level courses, master's degrees, and certificates in various areas within information assurance, but did not grant PhD degrees. Instead, students pursuing a PhD in other departments had the option of taking graduate level courses offered by IAC for a doctoral specialization in information assurance. The IAC was also accredited by NSA as the Center of Excellence in Cyber Defense Research.

Apart from traditional disciplines such as engineering, mathematics, and political science--other interdisciplinary areas such as information science also had a lot in common with cybersecurity. Information science as a research domain focused on areas related to retrieval, storage, dissemination, and protection of information. Since cybersecurity research was also concerned with the information protection, a few institutions offering information science terminal degrees also had a cybersecurity track. For instance, an information science PhD with a focus on information security offered by the School of Computing and Information at University of Pittsburg trained students to do research in deployment and design of secure information systems.

Amongst business schools, the Eller School of Management at the University of Arizona offered a PhD degree in Management Information Systems with a minor in Information Assurance. The minor requirement was determined by the department offering it. Hence, students were expected to take courses offered by the interdisciplinary center of information assurance. A minimum of nine credit hours of courses were required to be completed for fulfilling the minor requirements. More broadly, individual students enrolled in MIS PhD programs often had considerable latitude in choosing their own research focus. As a result, they could choose to direct their dissertation towards cybersecurity-related topics. In doing so, they could often qualify for cybersecurity faculty positions.

Business Doctorates

In the U.S., business doctorates could be acquired with two broad objectives in mind. The first, and most common, was to establish a career as an academic researcher. The second was to learn research methods so they could be applied to practice.

PhD Degrees in Business

The focus of traditional doctorates in business was to produce faculty members qualified to conduct research and teach in business schools. In the U.S., the earliest of these doctorates (the Doctor of Business Administration degree introduced by Harvard Business School) had an applied and interdisciplinary focus. The participants in these early programs normally entered only after having substantial careers as practicing managers.

By the 1960s, however, business doctoral education had started moving in a much more theoretical direction. Research disciplines built around the core business functions (e.g., management, accounting, finance, marketing and, later, information systems) began to appear. Business journals became increasingly specialized, and the creation of new theory became the researcher's ideal. With this change, the PhD—closely resembling its social science counterparts in economics, psychology, sociology, and decision science—became the typical (and preferred) degree for academic researchers. The programs most successful at placing graduates, offered by top research universities, had extremely competitive admissions standards, and required students to attend full-time. Commitment to business research—in the context of launching a full-time academic career—rather than commitment to business practice, was the guiding criterion for selecting students.

Executive Doctorates

Starting in the 1990s, a new type of business doctoral program began to emerge in the U.S. These programs were part-time and designed for executives with a minimum of 7-12 years of work experience. These programs bore some resemblance to professional doctoral programs that had earlier developed in the U.K. and Australia. The U.S. programs differed, however, in their heavy reliance on coursework and their use of cohort structures to move groups of students through the process at the same time. Most U.S. programs awarded the DBA degree, to distinguish them from traditional PhD programs. Others invented their own degree, such as Case Western Reserve University's (CWRU) Doctor of Management and Georgia State University's (GSU) Executive Doctorate in Business (EDB). Unlike the traditional PhD at a research university, these DBA programs allowed students considerable flexibility in dissertation research, residency requirements, external employment policy (with continuing to work through the program being encouraged) and plan of study. Most were interdisciplinary or multi-disciplinary in their focus. Nearly all emphasized the application of research to practice. Nor did they assume graduates would go on to pursue academic careers. Instead, many were expected to apply the research skills they acquired to their existing careers or professions. Some key differences between these programs and the traditional PhD are listed in Exhibit 4.

The first U.S. program using the executive doctorate model at a major research university was started by CWRU in Cleveland, Ohio. The program focused on designing sustainable systems and graduating candidates were expected to develop the ability to think critically about the problems confronting an organization, a community, a nation, and the world. By 2017 however, about 28 business schools (including USF) offered DBA programs across the U.S., with a similar number of programs appearing in Europe. The Executive DBA Council (EDBAC) formed in 2010 to serve as a platform for sharing experiences and providing guidance to other schools who wished to start or enhance a DBA program. In 2013, AACSB International, the premier accrediting agency for business schools, published a report titled: "The Promise of Doctoral Education" that was perceived to be quite favorable in its view of this

new category of program. Increasingly, it was acknowledged that the graduates of these programs could be effective in academic programs, should they choose to make the transition after they graduated. From the early experiences of DBA programs, it was evident that getting new students was not the principal problem facing these programs. In an interview, the program director of CWRU pointed out that even the rise in the tuition did not hinder quality students from applying to their program, the most expensive one in the nation. On the other hand, finding the right faculty for this program was a challenge. He noted that supervising executive doctoral students was a frustrating experience for some professors who were used to supervising regular graduate students. He also added that the faculties from other departments such as law, political science, or anthropology did well to meet the requirements of the DBA students. Similarly, at Georgia State University's business school, out of 200 full-time faculty, only 30-40 were reported to be a good fit for the program, and many chose to work with more malleable regular PhD students than participating in the program.

Within the U.S. executive DBA programs, a schism had started to develop regarding the appropriate goal for the programs. Some programs, such as that at CWRU, had increasingly come to target transition to academia and participation in the academic research community (through publication in top tier journals) as the outcome they most valued. In many respects, this put their graduates in competition with graduates of full-time PhD programs. Other programs, such as the USF Muma DBA, emphasized the application of research methods to practice; in these programs, publication was seen to be a secondary benefit.

University of South Florida

The Muma College of Business was one of several colleges on the Tampa campus of the University of South Florida. Located in Tampa, Florida—the west coast of the center of the state—USF was one of ten universities in the Florida state university system (SUS). The university has experienced remarkable growth since its founding in 1956. Among the facts and "Points of Pride" listed on its 2017 website, the school boasted:

- 49,000 students
- 3 campuses
- The USF System was awarded a record $458.5 million in contracts and grants in fiscal year 2016.
- The USF System ranked 9th in the nation among public universities and 21st world-wide for granted U.S. patents among all universities.
- The USF System ranked 45th in the U.S. for total research expenditures, among all U.S. universities.
- The USF System ranked 28th in the nation among public universities for total research expenditures.
- USF is classified as a Doctoral University with Highest Research Activity, a distinction attained by only 2.5% of all post-secondary institutions.
- USF led the U.S. in Core Faculty Fulbright awards in 2016.

Within the state, USF was classified as "emerging pre-eminent," making it eligible for additional funding to support its research and educational activities. It was expected to join the state's two "pre-eminent" universities—the University of Florida (UF) and Florida State University (FSU)—within the next few years, having already surpassed the latter according to most of the criteria established by the state for ranking its universities.

Strategic Goals

The strategic plan of USF emphasized four key goals (USF, 2017), defined as:

1) To produce well-educated and highly skilled global citizens through continuing commitment to student success.
2) To engage in high-impact research and innovation that changes lives, improves health, and fosters sustainable development and positive societal change.
3) To create a highly effective, major economic engine, creating new partnerships to build a strong and sustainable future for Florida in the global economy.
4) To have sound financial management to establish a strong and sustainable economic base in support of USF's continued academic advancement.

USF Colleges and Centers

USF Colleges at USF included Arts and Sciences, Behavioral and Community Sciences, Business, Education, Engineering, Marine Sciences, Medicine, Nursing, Pharmacy, and Public Health. Of these, Arts and Sciences was the largest, with the Muma College of Business being the second largest--with around 5,500 students according to its annual report. The university also had a number of colleges that offered selected programs across disciplines, including the Patel College for Global Sustainability, the Honors College, and the College of Graduate Studies.

Within colleges, specialized centers were often established. The university also had centers that worked across colleges, such as the Center for Entrepreneurship. Some USF centers even served the broader Florida SUS universities, as well working across colleges. A good example of such a center was the Florida Center for Cybersecurity.

Florida Center for Cybersecurity

In Florida, the SUS sought to make Florida the leading cyber state. To help accomplish this goal, the 2013 Florida Legislature called on the state's Board of Governors to submit a plan for the creation of the Florida Center for Cybersecurity (FC2), a shared resource for Florida's stakeholders in education, government, defense, and industry. This center was principally located at USF and worked in tandem with the USF and other SUS faculty.

The vision of the Florida Center for Cybersecurity (FC2) was to position Florida as the national leader in cybersecurity through education, innovative interdisciplinary research, and community outreach. (FC2, 2017). It's mission statements were to:

Create thousands of high-paying jobs in the state's cybersecurity industry.

- Serve as a facilitator for cybersecurity education.
- Enhance Florida's cybersecurity workforce, including reintegrating military veterans by utilizing their specialized skills and training.
- Act as a cybersecurity clearinghouse for statewide business and higher education communities to help mitigate cybersecurity threats, and optimizing investment to eliminate unnecessary duplication.
- Attract new financial, healthcare, transportation, utility, and defense companies to Florida.

The FC2 was a pan-Florida organization housed at/supported by USF. The choice of USF to host the center was motivated by a number of factors, including its size, emerging pre-eminence, and central location in the state. Particularly critical to the decision was USF's proximity to MacDill Air Force Base, which was the headquarters of two major military commands: U.S. Central Command (CentCom, which coordinated activities in particularly sensitive global regions, such as the Middle East) and U.S. Special Operations Command (SoCom, which coordinated activities of the special forces of each military service). Both active duty servicemen and women and veterans of the services played an active role in the cybersecurity industry. And there were few places where the concentration of these individuals was higher than in the Tampa Bay region.

At the time of the case, USF was working on a proposal to build a Sensitive Compartmented Information Facility (SCIF; pronounced "skiff") at USF. SCIF was a U.S. Department of Defense (DoD) term for a secure room, and it would be a highly secured data center with access limited to those individuals with appropriate security clearances and a need for entry. Were the SCIF proposal to be accepted and funded, there would obviously be more work of the Department of Defense (DoD) at FC2. This would mean more job opportunities for cybersecurity professionals and more visibility for USF's cybersecurity activities.

FC2 offered an online MS in Cybersecurity program, supported primarily by four colleges: Engineering (Computer Science), Behavioral and Community Sciences (Criminology), Arts & Sciences (Information Science), and Business (Information Systems and Decision Sciences, ISDS). Many of these colleges, including business, were also offering or preparing to offer undergraduate cybersecurity majors or minors. As well as having core course requirements, the MS degree had four distinct concentrations: Cyber Intelligence, Digital Forensics, Information Assurance, and Computer Security Fundamentals. Graduate certificate programs, requiring as few as four courses, were also offered. The information assurance concentration was already managed by the ISDS department. Should the Cybersecurity DBA program launch, it would become another program in cybersecurity administered through the Muma College of Business.

Muma College of Business

USF's Muma College of Business had around 5,500 students. In terms of enrollment, it was among the largest colleges at USF, second only to USF's College of Arts & Sciences. In addition to its SACS regional accreditation (shared with the university as a whole), its business and accounting programs were accredited by *AACSB International.* The college reported more than 150 faculty/staff and had an operating budget of around $19 million.

The college was organized into four main departments: the Lynn Pippenger School of Accountancy, Finance, Information Systems & Decision Sciences (ISDS), and Marketing. The largest programs offered by the college were its undergraduate programs in business and accounting. The college hosted a variety of centers, including the Center for Entrepreneurship, the Small Business Development Center (SBDC), the Business Communications Center, the Center for Supply Chain Management & Sustainability, and the Center for Analytics and Creativity. At the graduate level, the college boasted a wide range of programs, including doctoral degrees, disciplinary master's degree programs, an MBA program, and an Executive MBA program.

In the cybersecurity area, the ISDS department offered an undergraduate degree in Business Analytics & Information Systems (BAIS) with a cybersecurity concentration, supported by electives such as Information Security and IT Risk Management, Global Cyber Ethics, and Cybersecurity Cases. The department also offered cybersecurity-related courses in its MS-BAIS program, which had the largest enrollments of any MS degree offered by the college. The college also provided courses for the MS in

Cybersecurity offered by the FC2, and taught the curriculum associated with the Information Assurance concentration in that program, as well as the related certificate.

Dr. Manish Agrawal, chair of the ISDS department, had research specialties that included cybersecurity, and had published a textbook on information security. He had attended the same NSF PI conference where Gill had learned about the serious shortage of cybersecurity-qualified faculty. When Gill had speculated about the possibility of creating a specialized DBA cohort that focused on cybersecurity related research skills, he had been immediately enthusiastic. He had already seen that there was a huge demand for professionals in the cybersecurity area. He had also experienced the difficulty in hiring cybersecurity-qualified faculty. Colleges of business around the country were competing for these scarce resources. In addition, applicants coming out of computer science specialties were often ill-prepared to engage in the types of research that led to publications in the top-tier business research journals that were used as the basis for promotion and tenure. The department had already seen applicants turn down offers based on concerns that their research would not fit the college's requirements. These were growing ever more stringent as the prominence of the college continued to rise (see Exhibit 5).

The Muma DBA Program

The DBA program at the Muma College of Business was first launched in January 2015. At the time of its launch, it was the 11th AACSB-accredited part time executive doctorate in business in the U.S., and the fourth such program in the state of Florida. The positive response to the program far exceeded anyone's expectations, including Gill's. Both of the first two cohorts had exceeded enrollment targets by more than 50%—placing a considerable strain on available faculty resources in the college. The program had also quickly gained national attention. Indeed, the first national ranking of such programs—published by a little-known group in late 2015—had ranked the program as #1 in the U.S. out of the 50 programs listed. Gill had steadfastly refused to publish this ranking on the program's website, however. He thought privately that the program might well merit that rank in the future. But to rate a program so highly before a single candidate had graduated? Premature at best—and it left nowhere to go but down.

Admission Requirements

The admission requirements of the DBA program were weighted heavily towards practical experience. To receive preliminary acceptance, applicants needed the following:

- *12 years of professional work experience, at least 5 of which were at an executive or senior managerial level*. Gill and the DBA committee had already interpreted senior technical experience as meeting the 5-year requirement, since many of the program's applicants came from IT and other technical backgrounds. They were in the process of submitting changes to the graduate catalog to clarify the requirement.

- *An accredited undergraduate degree in any subject area, with a master's degree strongly preferred.* Thus far, the program had only admitted a couple of individuals that did not have a master's or equivalent graduate degree; in both cases, this decision was based on the quality and prominence of their work experience.

- *A completed DBA application.*

- *A statement of purpose*. This document was required to identify how the applicant felt the skills acquired in the DBA program would contribute to his or her future career.

- *An hour-long interview with members of the DBA Committee*. This committee contained a representative from each Muma department plus the program's Academic Director (Gill) and Director (Dr. Matt Mullarkey), and was responsible for program oversight.

Applicants were normally pre-screened by Mullarkey before the interview stage, so that the hundreds of inquiries made to the program did not result in hundreds of interviews.

In its interviews, the DBA committee emphasized that the program's goals were built around applying research to practice, rather than to act as the launching pad for a future academic career. Nevertheless, a small percentage of accepted applicants (under 20%) had already held post-professional academic positions. For this group, the Muma DBA offered an entry to a more attractive career path within academia, where properly accredited terminal degrees were considered vital to career advancement.

Curriculum

As just noted, the program was cohort based. It met ten times a year for two full-day residency sessions (Friday & Saturday). Between sessions, participants were expected to devote 10-15 hours a week to activities that were posted online. At the time of the case, the program had three cohorts enrolled, with the inaugural cohort scheduled to graduate in December 2017. Attrition rates in the graduating cohort had been quite low, of the 26 participants that started in 2015, 22 were on a path to graduate, and another had skipped a year and was now completing the program with the second cohort. In the second cohort, attrition had been even lower—with 37 starting the program and 35 of that group continuing as they approached the end of their second year.

As shown in Exhibit 6, the DBA program's structure was designed with maximum flexibility in mind. The first two years of the three-year program principally involved coursework in classes of four different types:

- ***Core Research courses (15 credits):*** These 5 classes were devoted entirely to teaching participants a wide range of qualitative and quantitative research skills that could be applied to address questions and decisions in practice.
- ***Special Topics courses (6 credits, changing to 12 credits):*** These 2 classes were selected based on proposals by research faculty who were interested in presenting topics related to their own research. At the time of the case, the two courses were Informing Science, taught by Gill, and Organizational Climate, a course taught by a faculty member from the College of Behavioral and Community Sciences.

- ***Strategic Focus courses (12 credits, changing to 6 credits):*** As the name suggested, these 4 classes were based on the areas of strategic focus for the college. At the time of the case, these included a course in Creativity and a course in Analytics, as well as courses in Ethics/Sustainability and in Strategy. Gill was in the process of getting approval to change the program's requirements, so that last two of these classes became Special Topics classes, providing the program with additional flexibility in incorporating faculty research interests.

- ***Publication courses (9 credits):*** These three classes involved participants developing a research paper that would be suitable for submission to publication, although such submission was not required.

Starting in October, the last quarter of the second year of the program, the structure of the program shifted. Participants, now referred to as candidates, met monthly in groups of four with their dissertation

committees for 4 hours in what were referred to as dissertation preparation courses (4 credits) and dissertation courses (16 credits). In parallel with these meetings, day-long 2-credit workshop courses, referred to as issues courses (10 credits) met on the remaining day of the residency. These issues courses were selected by the candidates themselves in the middle of their second year from a list of course proposals prepared by faculty. Thus far, the number of faculty proposals had been more than double the number of available slots (5).

The DBA program's dissertation process also offered a range of options. Candidates could fulfill the requirement with any of the following:

1. A standard dissertation
2. A collection of papers suitable for publication (usually three)
3. A practice-focused, research-informed book
4. A project and white-paper, intended for candidates who wished to create some sort of artifact, such as a software application, or whose project involved proprietary or classified activities
5. A portfolio of deliverables that had been approved by the committee

Gill knew of no other executive DBA program that offered this type of flexibility. But it was completely consistent with the program's philosophy. If its goal was to see research applied to practice, it needed to provide dissertation options that would fit the needs of candidates whose interests were more focused on applying research to solve business problems—as opposed to preparing research that would be suitable for publication.

Notably absent from the Muma DBA's curriculum were any courses focusing on research in a functional business discipline (e.g., management, marketing, accounting, finance, MIS). This omission was by design. From the initial stages of program design, Gill had always been adamant that the program should be interdisciplinary and should never attempt to teach participants the practice of business. It was the job of the DBA committee to ensure that participants came in with demonstrated knowledge of business practice. It was the job of the program to help them acquire the business research skills that faculty routinely applied throughout their academic careers.

A Cybersecurity DBA Concentration?

The idea of creating a separate DBA cohort specializing in cybersecurity had emerged during an NSF sponsored meeting for principal investigators (PIs) with grants in Secure and Trustworthy Computing (SaTC) area that took place in January 2017. Gill was the PI on such a grant—to develop a collection of cybersecurity case studies—and Agrawal, who was also attending, was one of his co-PIs. Throughout the three day meeting, three key points were repeatedly made:

1. That cybersecurity was intrinsically interdisciplinary.
2. That existing research was too heavily focused on the computer science side, and that more behavioral research was needed.
3. That the shortage of qualified cybersecurity faculty members with doctoral qualifications was becoming desperate.

At the end of a plenary speech that made precisely these three points, Gill had pulled Agrawal aside and pointed out that the DBA program was an interdisciplinary program that emphasized behavioral research and provided a fully-accredited doctorate in three years. He also pointed out that the program already had several participants who were already working in the cybersecurity area. Would it make sense to investigate the possibility of creating a version of the program specifically for cybersecurity professionals seeking a doctoral qualification. Agrawal, the chair of the ISDS department, immediately answered yes. And so began the investigation.

Fit with the DBA Program

The first question that needed to be addressed in considering the possibility of the cybersecurity DBA was if fit could be achieved. As Gill looked at the program closely, it became clear that the flexibility established to accommodate different business disciplines would work well for a cyber-security focused version of the program. He began by sketching out a rough draft of how the existing coursework would need to be modified. The draft is provided as Exhibit 7.

Particularly once the two "strategic area" courses had been changed to special topic courses, Gill's conclusion was that no changes to the program's overall course structure would be required. What would be required, for some courses, would be a change in content emphasis. For example, the informing science course that Gill taught focused on introducing transdisciplinary thinking; one major area of research in informing science that he currently skipped over was misinforming and disinforming. An emphasis on these would make the course much more relevant to security professionals. Similarly, the organizational climate course, already being taught as a special topics course, took a broad view of the factors that impacted behavior within the organization, such as policies and environment. Couldn't the issue of factors that impact security climate fit well within this topic area?

The flexible dissertation formats offered by the existing program also seemed to be a natural fit with a cybersecurity-focused program. When Gill had designed the project/white paper option for the program, he had originally viewed it as an option needed to accommodate proprietary research done on behalf of a company. The project would be kept confidential, the white paper would describe how the research methods were applied to the project. Within the existing DBA program, this option had already been used by members of the cohort that were developing software artifacts as the project. This option seemed tailor made to handle research that involved application development, or that was classified—a real possibility when military and veterans were program participants.

Indeed, as Gill thought about it, the only real modifications to the existing program would be related to admissions decisions. Whereas the existing program would accept any form of work experience that met its 12 year/5 year criteria, a cybersecurity cohort would only take those individuals will the same level of cybersecurity-related experience. This change to admissions criteria would, of course, be critical. Just as the regular DBA program did not teach business practice, the cybersecurity version would not teach cybersecurity practice. The participants would need to enter the program with those skills. The program's emphasis would be on developing research skills that could be applied to cybersecurity problems and decisions. Moreover, the modifications to admissions criteria would not really be a change. Otherwise qualified applicants that did not meet the cybersecurity experience criteria could always join the general DBA program—as could cybersecurity-qualified applicants interested in a general business research curriculum. The cybersecurity version would simply run independently, as an option, on separate weekends.

In considering the remarkable fit between the existing DBA program and the needs of a cybersecurity version, Gill came to a surprising conclusion. Since the regular and cybersecurity programs would be

identical in terms of requirements, there would be no obvious reason why approval outside of the Muma College of Business would be needed. Of course, needed and desirable were two different things.

Program Concerns

Before getting too enthusiastic about the possible cybersecurity program, Gill also realized that curricular issues were only part of the challenge. Where the real challenges were likely to lie was in the areas of institutional reaction, staffing, economics, and program focus. There was also the question of the degree to which existing DBA students would react positively to a new, parallel program.

Institutional Issues

Although it appeared that launching a new cohort under the auspices of the DBA program could be done with approval by the college, such a program would not go unnoticed by the university. As previously mentioned, the existing online MS in cybersecurity was offered under the auspices of the university's FC2. Gill was concerned about how they might react to a USF doctoral program in the cybersecurity area being offered outside of their control.

Beyond the FC2, Gill was concerned about the possible reaction of other colleges within the university. The colleges of Engineering, Behavioral and Community Sciences, and Arts and Sciences all had a significant stake in the growing number of cybersecurity initiatives. Surely, the need for a cybersecurity doctoral program had been noted by them. How would they react if the Muma College of Business launched one on its own initiative? While turf battles were regrettably common in universities, this one would be particularly concerning. The problem was one of staffing.

Staffing

The launch of a cybersecurity DBA program would have two significant implications for staffing. The first involved the availability of Muma faculty. In order to teach at the doctoral level, college policy—driven by accreditation requirements—demanded that all faculty members meet the highest research activity qualification: scholarly academic (SA). This had already led to two challenges for the existing program: finding the right SA-qualified faculty to teach in the program and ensuring that their teaching activities did not put them over the 25% limit on "overload" teaching specified by the university.

As a practical matter, this meant that relatively few of the researchers teaching in the existing DBA program could be pressed into service to teach in the cybersecurity DBA as well. That would mean that many of the faculty teaching in the new program would need to come from outside the Muma College of Business. Moreover, Gill anticipated that many of the special topics and issues courses in the proposed program would be more closely aligned with research techniques specific to some of the more technical issues of cybersecurity. In other words, the new program would likely need to draw heavily on faculty from outside the college.

The existing DBA program already made use of some faculty from outside the university and from other colleges, such as USF Health and the College of Behavioral and Community Sciences. Thus far, these relationships had worked splendidly. They were dependent, however, upon deans in each of the colleges involved giving permission for their faculty to teach in the program. What would happen, however, if those same colleges were to be unhappy that the Muma College of Business was launching a cybersecurity doctorate on its own? Where would the program find qualified faculty? Even if they did not object, how could the program be sure it was getting the *right* faculty? With their many years of practical experience, the participants in these programs could be quite demanding. Not all instructors reacted well to that type of pressure.

Program Economics

Whenever a new program was launched—even a modified version of an existing degree—initial enrollments were very difficult to predict. Historically, universities tended to overestimate the demand for new programs. In rare occurrences, such as the Muma DBA, the estimates were way too low. As a result, the program, which had initially been forecast to break even, had provided the college with some much needed funds for research and other expenses.

There was no certainty that a cybersecurity DBA would experience the same demand. At current tuition levels, Gill estimated that such a program would need at least 16 participants to break even. With fewer than that, it would likely drain any funds spun off by the existing program. Furthermore, that number might be higher, however, if it cannibalized applicants from the existing DBA program.

While state universities were not in the business of making money, only programs that could hold their own economically were likely to be sustainable. In addition, even if a program's launch were to be made contingent upon reaching a minimum cohort size, there would be a number of startup expenses associated with administration, marketing, and course development that would never be recouped in the event the program failed to launch. Gill estimated these expenses at several hundred thousand dollars.

One way of reducing the economic risk of a startup would be to acquire external funding. Given the desperate need for cybersecurity research faculty—particularly in the behavioral area needed by business schools—Gill thought such funding might be available. Indeed, the same SaTC program that had funded his case development might possibly be a source of up to $300,000 in funding for a new doctoral program. Other possibilities were NSF programs involving innovations in graduate education and workforce capacity building. The applicable portion of the NSF solicitation is provided in Exhibit 8.

While the possibility of getting funding was attractive, such funding sources were highly competitive, and they also took considerable time and effort to find, to create the proposal, and to learn of the resolution. For example, the SaTC program only took educational proposals once each year (in early December) and typically took at least 6 months to make its determination. Additionally, seeking funding left a key question unanswered: Did it make sense to go ahead with the project even if funding was not available?

Program Focus

Another concern of Gill's involved how the cybersecurity DBA might differ from the regular DBA in terms of its focus. He attributed part of the success of the original DBA to its laser-like focus: impart research skills that can be applied to practice. The goal was *not* to create more academic researchers.

While he anticipated a similar core focus for the cybersecurity DBA, there was no doubt that a significant part of the justification for it was the shortage of qualified faculty. That being the case, the program would probably need to shift slightly towards preparing participants to transition to academia. He wondered how this might impact the program. Just how large a modification would it entail?

Stakeholder Acceptance

The overarching concern Gill had was the likely reaction of key groups of existing stakeholders: the college and university faculty & administration, the leadership of FC2, and participants already enrolled in the DBA program. To acquire further insights into the likely degree of acceptance and/or resistance, Gill arranged for the case developers to meet with the head of the FC2, the dean of the Muma College of Business, and DBA participants currently working in cybersecurity-related fields. He also used an early draft version of the case for a classroom discussion with the second DBA cohort.

Interview with Sri Sridharan, Head of FC2

When the case writers approached Dr. Sri Sridharan who heads FC2, a few important things came to light. Dr. Sridharan corroborated Gill's observation that the demand for cybersecurity professionals was at an all-time high, and the supply came nowhere close to the needs. In the recent past, Sridharan recollected that FBI had approached him to recruit about 6000 cyber-intelligence professionals, and Sridharan could only say that there weren't so many professionals available. The FBI officials were looking for people who could get to the bottom of understanding the behavior underlying the people who commit cybercrimes, so that they could stem the issue at the root itself. Sridharan hinted that the cybersecurity DBA curriculum could include something in the field of behavioral analytics as the demand for the specialization was growing hugely.

When asked about the challenges in hiring good faculty, Sridharan sighed and explained the difficulty in getting good faculty to teach cybersecurity courses. He even joked saying that the search committee that had been formed to hire faculty was close to the end of tenure, and yet couldn't succeed in hiring the right faculty. Word-of-mouth was one of the ways to attract faculty, but the best way to get good ones, according to Sridharan, was to offer exorbitant salaries. This point was a matter of concern for Gill as it would inevitably increase the costs associated with the program.

Sridharan also pointed out an interesting observation that a lot of Ph.D. graduates in cybersecurity were attracted towards industry; far fewer chose the path of academia. Industry offered a lot of money as well as interesting challenges. Sridharan raised the possibility that most cybersecurity DBA graduates would prefer to continue working in industry rather than transition to universities. Apparently, the Board of Directors of many companies had been asking a lot of questions to the CIO, CEO, CFO, etc. about the steps taken to ensure the company's information systems were guarded against cyber-attacks. The senior executives of companies were now forced to understand the intricacies of cybersecurity, and Sridharan suggested that they could be potential students if the cybersecurity DBA gets introduced in the future.

On matters related to funding, Sridharan stated unequivocally that FC2 wouldn't be able to contribute anything in terms of dollars directly to USF, with an exception of a proposal for a grant which would again be evaluated by an independent committee. Applying for grants from Federal agencies like NSA or the Department of Defense had more chances of obtaining better results.

Sridharan concluded by saying that one of the challenges that he could foresee was the need to keep the curriculum up-to-date in a fast growing cybersecurity domain. He extended his organization's full support in helping with preparing the curriculum that stands in tandem with the latest market trends.

Interview with Moez Limayem: Muma College Dean

As the Dean of Muma College of Business at USF, Moez Limayem played a significant role in taking the college of business to the next level. In fact, it was Limayem who had launched the DBA program and was instrumental in making it a huge success. The DBA program was being recognized all over the U.S., and the program was slowly gaining a reputation as one of the best DBA programs across the country. It was a dream come true for Limayem, and he was quite happy to see the hard work of everyone involved in the program paying off.

However, when the case writers approached him regarding introducing a cybersecurity flavor of the existing DBA program, Limayem was quite skeptical of its success because of various reasons. With vast amount of experience in academia and being someone who trusts more in logic than intuition, Limayem expressed his concerns with the introduction of another parallel DBA program.

Firstly, though Limayem agreed with the fact that there was a huge demand in the cybersecurity area, he felt that the demand was more for the professionals who knew the technicalities of cybersecurity attacks and not for people at the senior management level. He wasn't sure if a DBA in cybersecurity would be of much help to professionals working in the cybersecurity area. Moreover, he also brought to light another important point that though the DBA is considered a terminal degree, a lot of research universities wouldn't really hire DBA graduates. Ph.D.s would be the ideal choice for universities offering tenured positions.

Secondly, Limayem made it very clear that it would be incredibly difficult to get faculty to teach another DBA course. Thus, on top of the fact that the existing faculty had already been stretched to the maximum, there was very little bandwidth left. Limayem didn't want the faculty to burn out from exhaustion as he explained that it would be counter-productive.

Thirdly, Limayem explained it would take a huge amount of financial investment to begin another program, and it involved a lot of startup costs. When asked if a grant would lend a hand, he said (personal communication, 2017):

> *A grant, even if it's very high, will run out after 2-3 years. What do I do then? Grant helps you seed money if you already have bandwidth. But if you really want a sustainable program that will stay and be one of the best in the country, you need continuous revenue.*

Limayem wanted to get a report on the feasibility analysis of the program primarily considering the bandwidth required. He was clear in his intention to start the program only if it was self-sustaining, like the existing DBA program. Limayem wasn't completely against introducing the new program, but he wanted to have a thorough analysis of the facts and statistics related to the demand and feasibility of the program.

Limayem also had an interesting recommendation to make. He was of the opinion that instead of starting a separate cohort for cybersecurity, a better option would be to let the existing DBA program remain intact for the most part and introduce a cybersecurity concentration of it by allowing the students to choose courses related to cybersecurity. This would solve almost all the problems that would occur by introducing another program. He was inclined to this option, but was also open to discussion. Overall, he needed data-backed answers to three important questions.

One, who would be the exact target audience of the cybersecurity DBA program and would they be willing to join? Two, why would anyone choose a cybersecurity DBA program? Three, why couldn't the existing DBA program be modified to accommodate and add a cybersecurity concentration instead of going down the painful process of creating a new program altogether?

Interview Findings

The case writers interviewed DBA students with experience in the cybersecurity arena to get their perspective about the cybersecurity DBA program. The response was that there were very few programs for cybersecurity DBAs, and a program in that domain would have a lot of demand and would be immensely useful to cybersecurity professionals.

An Interviewee, with 12 years of experience in the cybersecurity domain, indicated that the proximity of FC2 to USF and also to various military bases would be of great advantage for this program, and any collaboration with FC2 or Department of Defense would become a win-win situation for everyone. He

said that if he had to do it again, he would undoubtedly choose to join the cybersecurity DBA program as it would give him a distinct advantage.

A few of the other points mentioned were that the demand for cybersecurity professionals with behavioral expertise had been booming, and it was the right time to introduce a program like the cybersecurity DBA. The case writers were told that cybersecurity couldn't be considered as something to be learned in silos. For every technology company that uses IT solutions, the scope of cybersecurity spans throughout the organization. It was slowly becoming imperative to higher management personnel to learn and under various aspects of cybersecurity. For those people, the cybersecurity DBA program could offer what they had been looking for. Even companies wouldn't mind sponsoring their employees for such a program as it would benefit them in the long run. Company CxOs (e.g., CIOs, CEOs, COOs, CFOs) would need to have the capability to understand the threats and challenges posed to the organization in the form of cybersecurity attacks.

Other points made were that many cybersecurity personnel would show interest in academia after their retirement, and a DBA program would give them an edge over other qualifications. Also, owing to the short course duration of 3 years in comparison to the usual 5-year PhD, the DBA program could attract more people who just would like to have a terminal degree and utilize their vast experience in the field of cybersecurity. Also, the degree would help them grow and move across the organizations--both horizontally and vertically.

Interviewees were of the opinion that cybersecurity needs to be ingrained in everything that companies do. And sooner or later, the scope and implementation of cybersecurity in an organization would grow in prominence.

Case Discussion Results

Gill wanted to get some feedback about the cybersecurity DBA program to get a different view/perspective about the program. So, he decided to discuss the draft version of the case with the existing DBA students and tried to get their opinions. Since all the students of cohort had at least twelve years of work experience, with at least five years as an executive or senior-level manager, their views would carry some weight and could be useful in understanding the market for cybersecurity better.

The case-discussion started, as usual, with Gill asking any of the students to summarize the case for the class. A student of the DBA program, who also worked as an instructor, started talking about key points of the case. Gill wrote four important points on the board that would need to be discussed: viability of the program, support of external funding, bandwidth of faculty, and closing silos (among different departments).

The discussion revolved around these four aspects, and many interesting points were raised by the students. Firstly, regarding viability of the program, almost all the students opined that there was a demand for cybersecurity, and that a cybersecurity DBA program would attract a lot of professionals. They also felt that studying the behavioral aspects of cybersecurity was quite important. One of the key aspects of discussion about the viability of the program was that the cybersecurity domain was intrinsically a multi-disciplinary area, and it needed coordination among the faculty from various disciplines. Gill explained to students how different departments don't play well with each other, and how it was going to be difficult to bring them all together. This was one challenge that wasn't on top of the priority list, but was important nevertheless.

Regarding getting funds for the program, the discussion was about how most grants given by NSF went to the Computer Science Departments. Most professionals at the helm of NSF were from computer science, and hence they preferred granting funds to programs that dealt with the technical aspects of cybersecurity. But when Gill went to the NSF meeting, he realized that the discussion focused on the behavioral aspects of cybersecurity, and this could be considered a positive approach to receiving external funding in the future, should the Muma College of Business decide to launch the program.

The discussion was filled with different sets of opinions and a lot of interesting questions were asked by the students. Why start a new cohort instead of adding a cybersecurity concentration to the existing DBA program? Can the DBA program be extended to 4 years with the last year dealing only with the cybersecurity domain? Would such a program be able to attract students, or would 4 years be too much? Should USF consider running 3 cohorts at a time or 1 cohort? What would be the pros and cons of taking up such an approach? How should one evaluate research of an interdisciplinary program like the cybersecurity DBA? Would cybersecurity DBA professionals want to go to academia or industry? What would the curriculum be like? And there were many more questions.

Gill thought that all the questions were important, and he felt that he needed clear answers to the questions, so as to get a better idea of how the program should be structured. This was the very reason why he wanted to have a discussion with DBA students in the first place, and it seemed like the discussion was indeed fruitful. He now needed to delve a bit deeper in those questions and understand the risks better as well.

A survey was circulated after the discussion, and 31 students participated in it (see Exhibit 9). One of the interesting findings from the survey was that while almost all the students agreed that there was a huge demand for cybersecurity, and a cybersecurity DBA would definitely attract a lot of professionals, none of them had heard of or known anyone from a cybersecurity DBA program. Most of the students considered taking the path of academia after the DBA program, sooner or later. It could be safely assumed that a lot of cybersecurity DBA graduates would like to take the same path as well.

The Decision

As he considered the options available to him, Gill recognized that the decisions to be made did not really belong to him. Instead, his role would be to make a recommendation to the college dean and to the faculty. Nevertheless, should the decision be made to go forward, he would likely play a critical role in the program's implementation. That being the case, he wanted to be sure that the odds of a success were as high as possible. He pondered what to recommend:

- Should the whole idea be dropped at once? The existing DBA was going well. Was it worth taking the risk of disrupting it with a new parallel program?
- What other sources of information should be tapped prior to making the decision?
- If the decision was to go ahead, should it be made contingent upon acquiring external funding?
- To what degree should the FC2 be involved in the program planning and implementation, if at all?
- To what degree should other colleges be consulted in the launch of the program?

The decision was not without time pressure. If a grant proposal for startup funding was to be made, the SaTC program deadline was early December; other potential program deadlines were as early as mid-October. If these deadlines were missed, then he would likely have to wait an entire year prior to seeking any external funding.

References

Collins, J. W., Soo Hoo, T. Y. B., Krantz, M., & Cosgrove, R. (2012). Creating an executive doctorate in civil security in the United States. *Journal of Homeland Security and Emergency Management*, *9*(2).

FC2. (2017). *Mission: Florida Center for Cybersecurity (at USF)*. Retrieved from http://thefc2.org/about-us/mission.aspx

Morgan, S. (2015, December 20). Cybersecurity market reaches $75 billion in 2015; Expected to reach $170 billion by 2020. *Forbes.* Retrieved from https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#46c3a87f30d6

NICCS. (2017). *The national initiative for cybersecurity education (NICE) cybersecurity workforce framework.* Retrieved from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

NSA. (2016). *National centers of academic excellence in cyber defense*. Retrieved from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

Raposa, M. (2017, February 12). Hacking increase sparks more cybersecurity programs. *The Washington Times.* Retrieved from http://www.washingtontimes.com/news/2017/feb/12/hacking-increase-sparks-more-cyber-security-progra/

Raytheon. (2015). *Securing our future: Closing cybersecurity talent gap*. Retrieved from http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_278208.pdf

Shoemaker, D. & Kohnke, A. (2016). Cyber education and the emerging profession of cybersecurity. *EDPACS*, *54*(5), 12-16. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/07366981.2016.1229984

USF. (2017). *The 2013-2018 strategic plan.* Retrieved from http://www.usf.edu/provost/documents/strategicplan-usf/usf-strategicplan-2013-2018.pdf

Acknowledgements

This case study is based upon work supported by the National Science Foundation under Grant No. 1418711.

Biographies

Utkarsh Shrivastava is a doctoral candidate in the Information Systems and Decision Sciences department at the University of South Florida in Tampa, Florida. He also has a Bachelor's degree in Information Technology and an MBA from Indian Institute of IT & Management. His research interests include health information technology, statistical data mining, ICT for development, and cyber security. He has taught systems analysis and design and applied data science courses to undergraduates at USF. Utkarsh likes to travel and present his work at research conferences in the information systems and business analytics domain.

Taufeeq Ahmed Mohammed is a student at University of South Florida, doing his Master's in Business Analytics and Information Systems. While pursuing his interests in the field of Data Analytics and Decision Sciences, he also works as a Teaching Assistant and a Graudate Assistant, teaching undergraduates and writing business case studies respectively. He considers himself as a creative data scientist in the making. He is also a published author of a narrative non-fiction book and a commercial fiction book, and he intends to write more books in different genres in the near future.

Exhibit 1: Email to Moez Limayem from Grandon Gill

1/21/2017

Moez & Manish:

The EE chair just asked me to participate in another NSF proposal. When I saw the solicitation, however, I realized that we might use one of the programs as a launching pad for the DBA. We cannot do it this year—since the due date for the letter of intent has already passed—but if the solicitation is renewed next year, the "NRT Innovations in Graduate Education (IGE) Track" provides up to $500,000 over 3 years for innovative interdisciplinary STEM programs. (FYI, cybersecurity qualifies as an "other interdisciplinary research theme of national priority").

With that kind of seed money, we could launch the cybersecurity DBA and cover the startup costs, most of the instruction costs and offer substantial scholarships so that even if we only had a tiny cohort, we could (at least) break even.

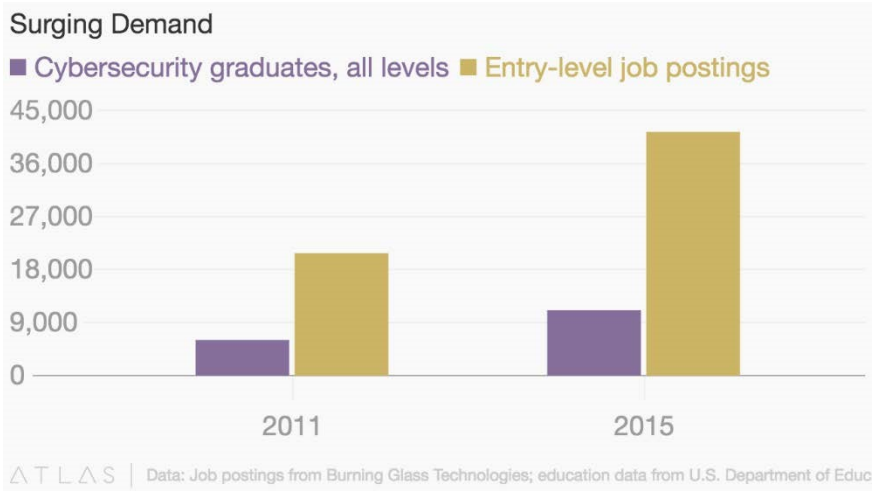
This year's solicitation can be found at: https://www.nsf.gov/pubs/2016/nsf16503/nsf16503.htm

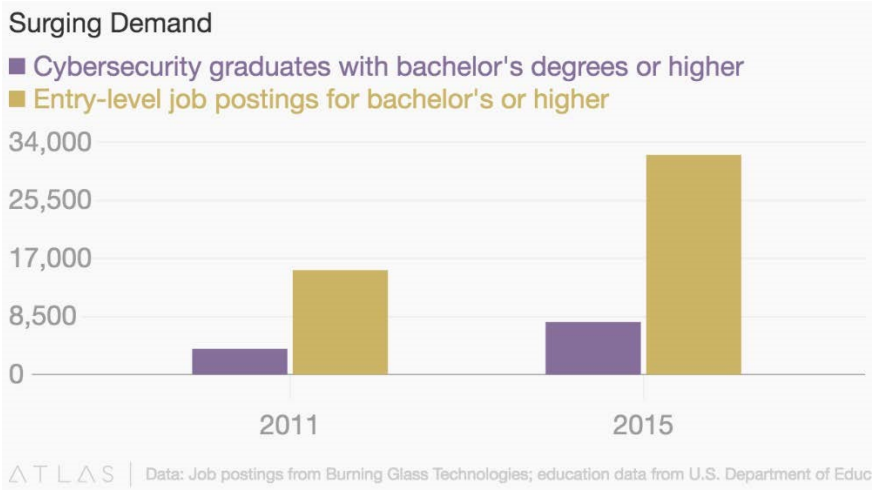
Again, nothing we can do this year. If we wanted to propose this fall, however, we would want to have all the elements in place so that we could launch the cybersecurity cohort if the proposal were funded.

Regards,

Grandon
T. Grandon Gill, DBA
Professor and DBA Academic Director
Information Systems & Decision Sciences Department
CIS1040
Muma College of Business
University of South Florida
4202 E Fowler Ave.
Tampa, FL 33620

Exhibit 2: Demand and Supply of Cybersecurity Graduates





Source: http://www.chronicle.com/article/Cybersecurity-Rising/239270

Exhibit 3: Computer Science PhD in Cybersecurity (ASU)

Arizona State University (ASU) Degree Requirements: 84 credit hours, a written comprehensive exam, an oral comprehensive exam, a prospectus and a dissertation

Required Core Areas (15 credit hours)
architecture and networked systems (3)
intelligent and interactive systems (3) data
and information systems (3) software and
information assurance (3) foundations of
computation and algorithms (3)

Other Requirement (6 credit hours) six
additional credit hours in one core area (6)

Electives (33-39 credit hours)

Research (12-18 credit hours)
CSE 792 Research (12-18)

Culminating Experience (12 credit hours)
CSE 799 Dissertation (12)

Ph.D. Concentration (Information Assurance) Requirements:
The program requires 30 credit hours, comprised of the following components:
9 credit hours from the three core areas (3 credit hours from each):

- Foundations (3)
- Systems (3)
- Applications (3)

12 credit hours from the Concentration Courses:

- CSE 539: Applied Cryptography (3)
- CSE 543: Information Assurance and Security (3)
- CSE 545: Software Security (3)
- CSE 548: Advanced Computer Network Security (3) 3 credit hours of Concentration electives:
- CSE 466: Computer Systems Security (3)
- CSE 467: Data and Information Security (3)
- CSE 469: Computer and Network Forensics (3)
- CSE 531: Distributed and Multi-Processor Operating Systems (3)
- CSE 534: Advanced Computer Networks (3)
- CSE 565: Software Verification, Validation, and Testing

6 credit hours of CSE 599 – Thesis

Culminating Experience: Defense

Source: Arizona State University website

Exhibit 4: Comparing Traditional and Professional Doctorates

Attribute	Academic PhD	Professional Doctorate
Domain of research topic	Disciplinary theory	Professional practice
Research type	'original investigation undertaken to gain new knowledge and understanding but not necessarily directed towards any practical aim or application' (p. 71)	Issues of real interest to the profession
Research focus	A perceived gap in the literature	A problem encountered in practice
Starting point	Finding what is known in the literature	A problem for which the solution is unknown
Intended learning outcomes	Contribution to the literature	'A significant original contribution to knowledge of practice
Integration of practice/theory	Low	High
Research outcomes	Long dissertation	Shorter dissertation, often more than one; project reports
Breadth	Narrowly focused	More broadly focused, problem-driven

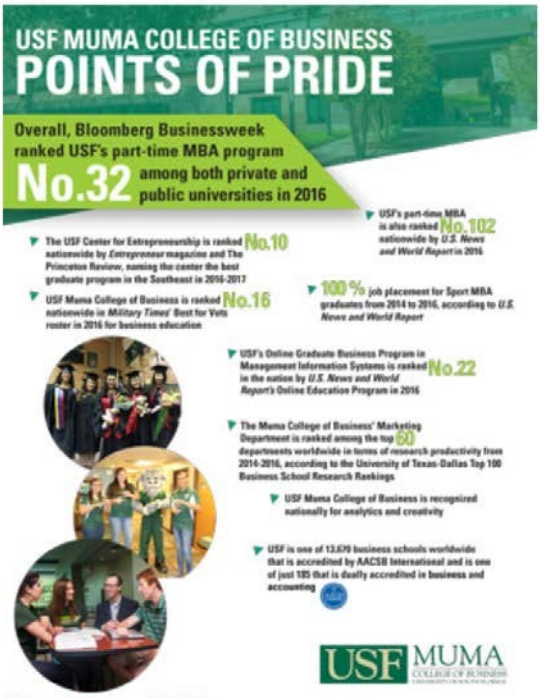
Attribute	Academic PhD	Professional Doctorate
Career focus	Entry into academia	Address the career needs of aspiring professionals
Entry qualification & degree	Undergraduate degree with high marks	A Master's degree is often required
Experience requirement	None	1-5 years usually expected, with a median of 3
Taught component	Minimal, under the "traditional PhD model"	Ranges from 15 to 50% of degree requirement
Modularity	Relatively unstructured according to the "traditional PhD" model	Modular course and credit structure
In-service vs. Pre-service	Pre-service for research career	In-service for professional career, often taken while working
Mode of study	Full-time	Part-time
Integration of work/study	N/A	High
Cohorts	No	Yes
Variability of duration	Very high	Low
Assessment	Dissertation driven	Separately assessed components

Source: USF College of Business Department Chairs Meeting Presentation, Fall 2012.

Exhibit 5: Muma College of Business "Points of Pride"

Points of Pride

The USF Muma College of Business boasts one of the nation's best accounting schools, a top-ranked entrepreneurship center, a nationally-ranked MBA program, and world-class research faculty. The USF Muma College of Business and Lynn Pippenger School of Accountancy are separately accredited by AACSB International - the Association to Advance Collegiate Schools of Business. The hallmark of excellence in business education, AACSB's Board of Directors reaffirmed USF's accreditation in 2013, one of just 185 institutions worldwide certified for quality in both overall business and accounting programs. Overall, Bloomberg Businessweek ranked USF's part-time MBA program 32nd in the nation among both private and public universities in 2016. The USF Muma College of Business is ranked No. 16 nationwide in Military Times' Best for Vets roster in 2016 for business education. Our Center for Entrepreneurship is ranked No. 10 nationwide by *Entrepreneur* magazine and the *Princeton Review*, naming the center the best graduate program in the Southeast in 2016-2017.



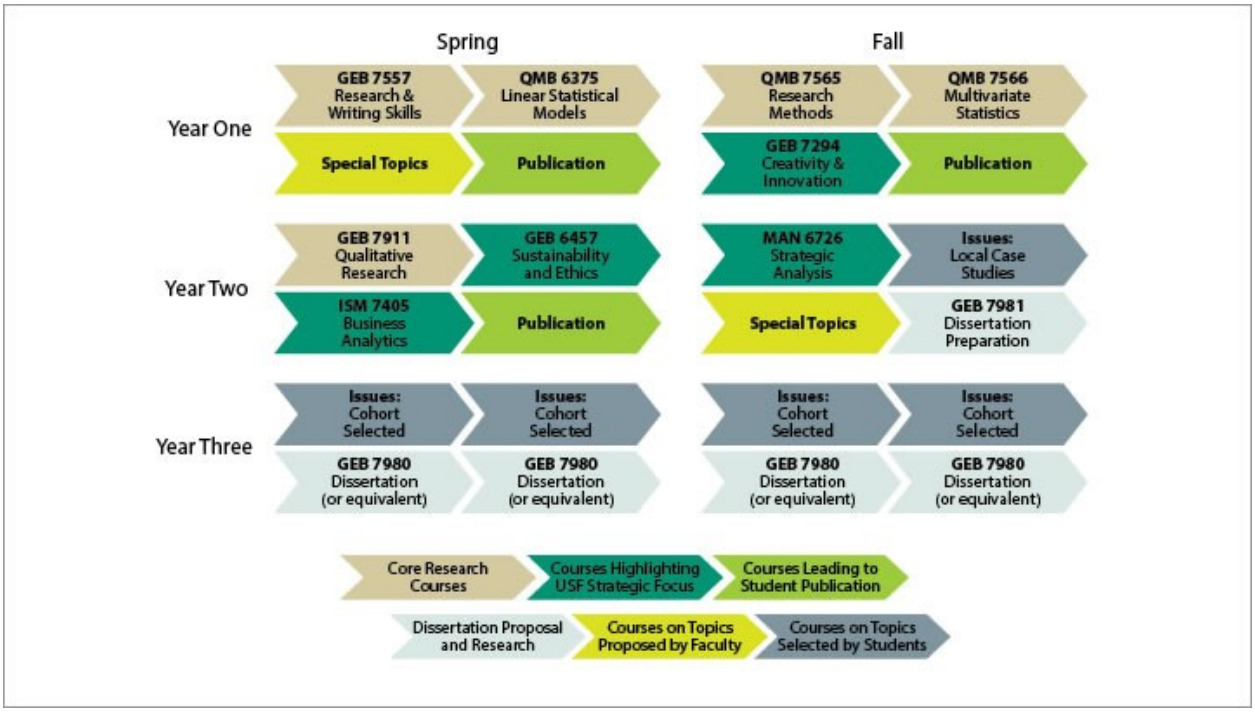
View Points of Pride
View Factsheet

Recent Rankings

- The University of South Florida part-time MBA program is also ranked No. 102 nationwide by *U.S. News and World Report* in 2016.
- USF's Online Graduate Business Program in Management Information System is ranked No. 22 in the nation by U.S. News and World Report's Online Education Program in 2016.
- The University of South Florida's Center for Entrepreneurship was the only Florida school on the list of the **nation's best entrepreneurship education programs for 2016- 2017**. The rankings have placed the center in the top 25 for the past 10 consecutive years.
- According to U.S.News and World Report, there is 100% job placement for Sport MBA graduates from 2014 to 2016.
- The Muma College of Business' Marketing Department is ranked among the top 60 departments worldwide in terms of research productivity from 2014-2016, according to the University of Texas-Dallas Top 100 Business School Research Rankings.

Source: http://www.usf.edu/business/about/points-of-pride.aspx

Exhibit 6: USF DBA Structure



Source: http://www.usf.edu/business/graduate/dba/curriculum/

Exhibit 7: Gill's Possible Modifications to DBA Courses

Course	Objectives	Modifications for Cybersecurity
Research Skills	Core: Participants learn to use the library to search and acquire business research; learn about different types of publications	Expand content to cover common cybersecurity outlets (such as IEEE and ACM)
Informing Science	Special Topics: Participants learn about transdisciplinary research approaches and different perspectives on informing	Emphasize research into misinforming and disinforming
Applied Linear Models	Core: Participants learn basic statistical techniques and multiple regression	No changes needed
Publication I	Publication: Participants learn to develop discussion cases	Participants develop cybersecurity discussion cases
Creativity and Innovation	Strategic: Participants learn techniques for enhancing and researching creativity	Creativity is examined in the context of black hat and white hat hacking
Research Methods	Core: Participants learn research methods and experimental design most commonly applied in the behavioral sciences	No changes needed
Multivariate Statistics	Core: Participants learn a collection of advanced statistical techniques such as logit, cluster analysis, partial least squares	No changes needed
Publication II	Publication: Participants prepare a research article suitable for submission.	Increased emphasis on possible cybersecurity outlets and conferences
Qualitative Research	Core: Participants learn a variety of techniques employed in qualitative research, such as case research, ethnography and action research	Draw more examples from cybersecurity, such as the use of textual analysis on social media and other sites
Business Analytics	Strategic: Participants learn techniques for extracting useful information out of big data	Acquire examples and exercises using system and network data
Organizational Climate	Special Topics: Examine research on how factors such as policies and the environment affect employee behavior	Focus on how the climate is likely to impact individuals
Special Topics 3 & 4	Special Topics: Courses proposed by instructors in their research areas	Seek out instructors doing cybersecurity research from other colleges, such as engineering
Issues Courses 1 through 5	Issues: 2-credit workshop courses selected by the cohort based on proposals from faculty	Solicit proposals from faculty outside the college of business

Source: Developed by Grandon Gill

Exhibit 8: Summary of Two NSF Solicitations

Cybersecurity Education (EDU) Designation

On occasion, the results of SaTC-funded research lead to widespread changes in our understanding of the fundamentals of cybersecurity that can, in turn, lead to fundamentally new ways to motivate and educate students about cybersecurity. Proposals submitted to this designation leverage successful results from previous and current basic research in cybersecurity and research on student learning, both in terms of intellectual merit and broader impacts, to address the challenge of expanding existing educational opportunities and resources in cybersecurity. This might include but is not limited to the following efforts:

- Based on the results of previous and current basic research in cybersecurity, define a cybersecurity body of knowledge and establish curricular recommendations for new courses (both traditional and online), degree programs, and educational pathways leading to wide adoption nationally;
- Evaluate the effects of these curricula on student learning;
- Encourage the participation of a broad and diverse population in Cybersecurity Education;
- Develop virtual laboratories to promote collaboration and resource sharing in Cybersecurity Education;
- Develop partnerships between centers of research in cybersecurity and institutions of higher education that lead to improved models for the integration of research experiences into cybersecurity degree programs;
- Develop and evaluate the effectiveness of cybersecurity competitions, games, and other outreach and retention activities; and
- Conduct research that advances improvements in teaching and student learning in cybersecurity and, where possible, focuses on broadening participation.

Cybersecurity Education proposal budgets are limited to $300,000 and their durations are limited to two years.

Source: NSF SaTC Program Solicitation 16-580

Innovations in Graduate Education (IGE) Program

Synopsis of Program:

The Innovations in Graduate Education (IGE) program is designed to encourage the development and implementation of bold, new, and potentially transformative approaches to STEM graduate education training. The program seeks proposals that explore ways for graduate students in research-based master's and doctoral degree programs to develop the skills, knowledge, and competencies needed to pursue a range of STEM careers.

IGE focuses on projects aimed at piloting, testing, and validating innovative and potentially transformative approaches to graduate education. IGE projects are intended to generate the knowledge required for their customization, implementation, and broader adoption. The program supports testing of novel models or activities with high potential to enrich and extend the knowledge base on effective graduate education approaches.

The program addresses both workforce development, emphasizing broad participation, and institutional capacity building needs in graduate education. Strategic collaborations with the private sector, non-governmental organizations (NGOs), government agencies, national laboratories, field stations, teaching and learning centers, informal science centers, and academic partners are encouraged…

II. PROGRAM DESCRIPTION

IGE projects will generate potentially transformative models for improvements in graduate education that prepare the next generation of scientists and engineers for the full range of possible STEM career paths to advance the nation's STEM enterprise. IGE is dedicated solely to piloting, testing, and validating innovative approaches to graduate education and to generating the knowledge required for the customization and implementation of the most successful, transformative ones. The primary target population for IGE projects must be master's and/or doctoral STEM students in a research-based degree program that requires a thesis or dissertation.

The IGE program will not focus on comprehensive training (see NSF Research Traineeship Solicitation 16-503) or foundational research examining how graduate students learn (see EHR Core Research Solicitation 15-509), but rather will promote targeted test-bed efforts that are informed by evidence, including findings from research on learning.

Activities proposed as part of the research project may include, but are not limited to, student professional skill development, career preparation and vocational counseling, faculty training, inventive partnerships, international experiences, internships, outreach, virtual networks, and mentoring. In addition, projects should utilize evidence-based strategies to broaden participation of students from diverse backgrounds.

Goals of the IGE Program are to:

Catalyze rapid advances in STEM graduate education broadly as well as those responsive to the needs of particular disciplinary and interdisciplinary STEM fields, and

Generate the knowledge base needed to inform the development of models as well as their implementation and adaptability.

The IGE Program calls for proposals to:

- Design, pilot, and test new, innovative and transformative approaches for inclusive STEM graduate education;
- Examine the potential to extend a successful approach developed in one discipline or context to other disciplines, or transfer an evidence-based approach to a new context; and
- Develop projects that are informed by learning science and the existing body of knowledge about STEM graduate education.

- Leadership teams (PI/Co-PIs) comprising professional expertise in the learning sciences and pedagogy, as well as in the principal science domain(s), are strongly encouraged.

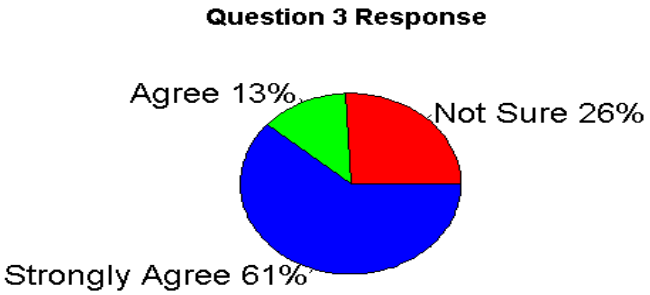
Source: NSF Program Solicitation 17-585

Exhibit 9: Student Survey Results

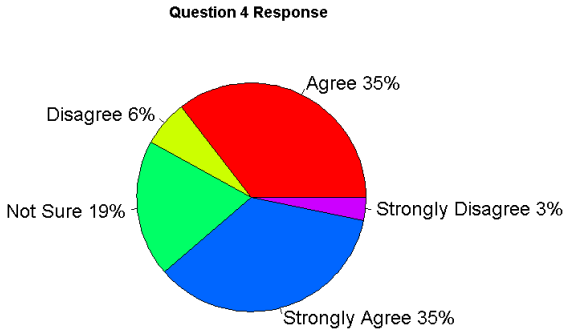
1. Have you ever heard of an executive business doctorate with cybersecurity focus? (Yes/ No)
   Response: No (100%), Yes (0%)

2. Have you ever met or do you know of anyone who has received an executive business doctorate or formal doctorate in cyber security? (Yes / No)
   Response: No (100%), Yes (0%)

3. Given the increase in the number of cyberattacks on companies, do you think the companies should encourage their CIOs, CXOs and CFOs for cyber security education?

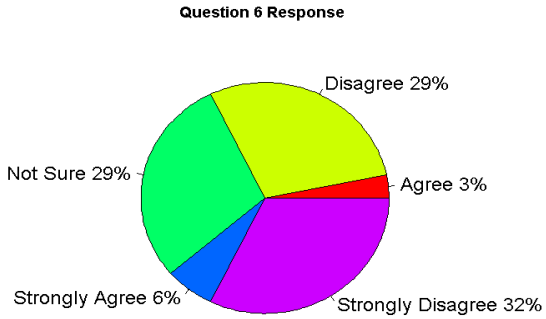


4. Do you agree that an executive doctorate with cyber security focus would be attractive for industry professionals with experience in cyber security area?

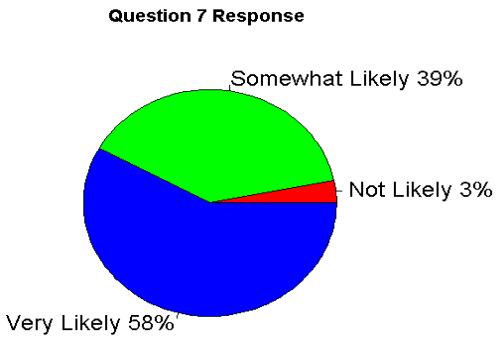


5. How satisfied are you with the current cohort size of the DBA program?

6. Do you agree that there is room for increasing the cohort size (by up to 10-15) without compromising with the quality of teaching, research and service to the students? (719x578)



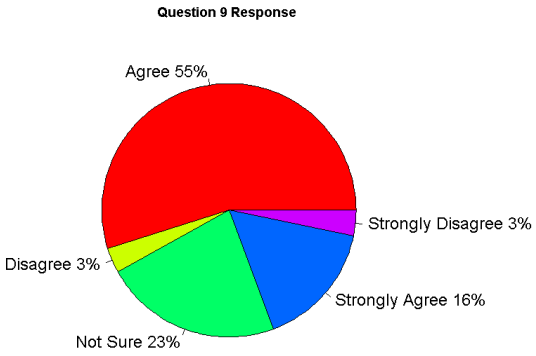
7. Have you ever thought about pursuing career in academia after completion of your DBA degree? Given a suitable choice how likely is it that you will pursue a career in teaching? Please check the appropriate box.



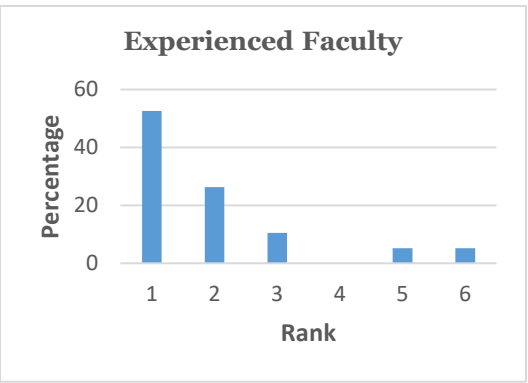
8. Do you have professional experience in areas of cyber security such as information assurance, information security, cyber forensics etc. If yes, then please specify the duration in years. (Yes / No)

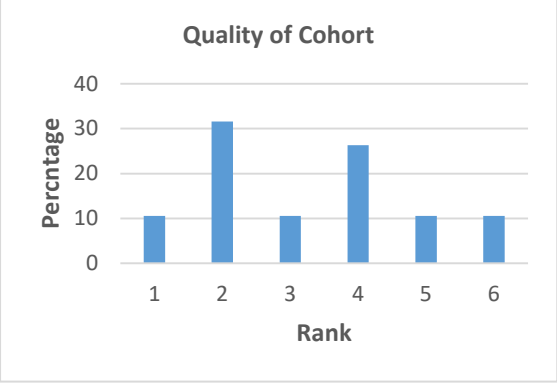
   Response: Yes (16%), No (84%)

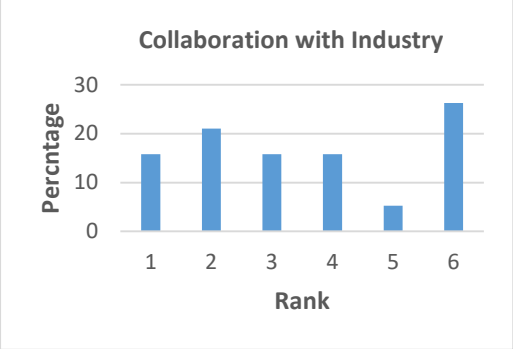
9. Do you agree that cybersecurity focused executive doctorate cohort would be attractive to professionals?

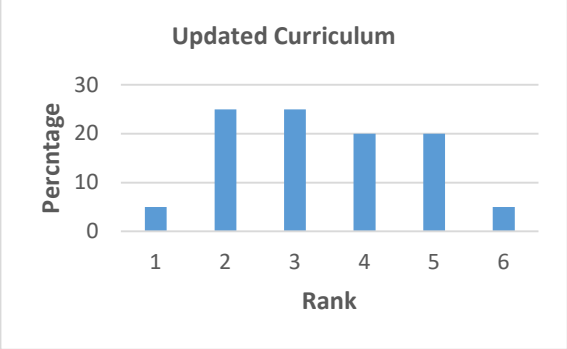


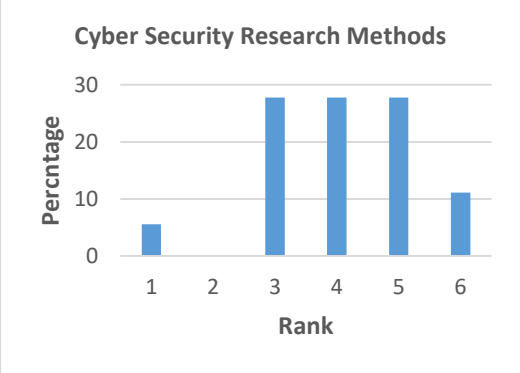
10. According to you, what's more important for the cybersecurity DBA program to succeed? Rank the items below in order.



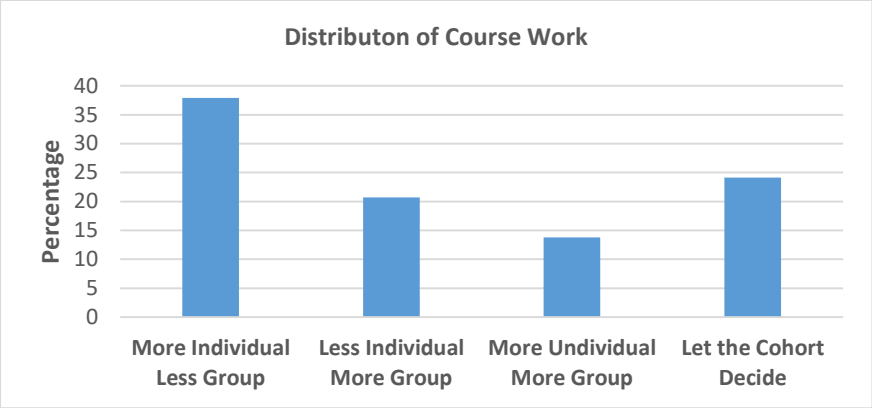








11. In terms of distribution of work related to the course, how much work do you think should be individual-based and how much should be group-based?



12. Would you like us to contact you if the EDB (cybersecurity) program moves forward?

(We will not use your contact information for any other purpose)

Response: Yes (20%), No (80%)
If yes, please provide us with your email address:

12. First Name:

13. Last Name:

14. Would you be willing to attend a focus group on how we might structure and market such a program? (Yes / No)

Response: Yes (25%), No (75%)

Source: Compiled by case writers