



**UNIVERSITY OF GUAM
UNIBETSEDÁT GUÅHAN
Board of Regents**

Resolution No. 20-36

**RELATIVE TO APPROVING THE UNDERGRADUATE MINOR AND CERTIFICATE PROGRAMS
IN CYBERSECURITY MANAGEMENT**

WHEREAS, the University of Guam (UOG) is the primary U.S. Land Grant institution accredited by the Western Association of Schools and Colleges Senior College and University Commission serving the post-secondary needs of the people of Guam and the region; and

WHEREAS, the governance and well-being of UOG is vested in the Board of Regents (BOR);

WHEREAS, UOG desires to establish a new undergraduate certificate program in Cybersecurity Management, as well as a Cybersecurity Management minor under the Criminal Justice program, under the direction of the School of Business and Public Administration (SBPA);

WHEREAS, Cybersecurity threats are a growing concern not only on Guam, but throughout the region and the world, and qualified information systems experts are needed to support existing infrastructure and expanding technology needs;

WHEREAS, UOG has the responsibility to lead the Western Pacific Region in meeting these challenges by offering a program that addresses the most critical needs faced by the region and the island;

WHEREAS, these proposed programs add a modest five courses to the curriculum; there are many qualified faculty with the expertise to teach in these programs in the division of Public Administration and Legal Studies (PALS); there are sufficient library resources for the programs; and there are available computer labs, Information Technology equipment, and support staff to support student learning;

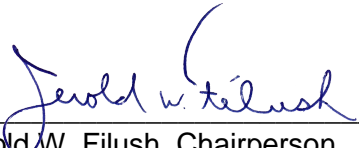
WHEREAS, a program demand report documents very high level of interest in the program, especially the professional certificate from respondents employed by Government of Guam agencies, such as Guam Department of Education, Department of Administration, Guam Economic Development Agency, Guam Police Department, Guam Fire Department, Department of Public Works, Guam Homeland Security, Veteran's Affairs; the Federated States of Micronesia government; professional organizations like Nisag'a data systems, Guam Power Authority, Pacific Human Resource Services, Zan Administrative Services, and Guam SurgiCenter; Pacific Islands Club and Sheraton hotels; the Army and Air National Guard; and educational institutions such as the Guam Community College, UOG, and the University of Glasgow;

WHEREAS, the proposed minor and certificate programs in Cybersecurity Management was prepared and submitted by the faculty in the PALS division; considered and recommended by the SBPA Academic Affairs Committee and Dean, endorsed by Undergraduate Curricula Review Committee and the Faculty Senate, and reviewed and recommended for approval by the Senior Vice President & Provost and the President; and

WHEREAS, the Academic, Personnel and Tenure Committee has reviewed the proposal and recommends to the BOR for approval the minor and certificate programs in Cybersecurity Management.


NOW, THEREFORE, BE IT RESOLVED, that the BOR hereby approves Cybersecurity Management certificate and minor programs, effective AY2020-2021.

Adopted this of 24th day of November, 2020.



Jerold W. Filush, Chairperson

ATTESTED:



Thomas W. Krise, Ph.D., Executive Secretary

University of Guam

Request for Official Action on a Policy or Regulation

- Date of this request:** 10/22/2020
- Destination of request:** (as per governance guidance or manual)
 Board of Regents President SVP&P VPAF/CBO Other _____
 BOR Committee: Academic, Personnel, and Tenure Budget, Finance, Investments, and Audit
 Physical Facilities Student Affairs, Scholarship, Alumni Relations and Honorary Degree
- Originating organizational unit:** School of Business & Public Administration
- Action proponent name:** Annette Santos, Dean email: atsantos@triton.uog.edu phone: _____
- Action requested:** Create a Cybersecurity Management Program
- Justification supporting action request:** See attached
- Requested effective date of action, if approved:** AY 2020 - 21

- Manual or document to be altered:**

| | |
|--|--|
| <input type="checkbox"/> BOR Policy | <input type="checkbox"/> RFK Library or MARC |
| <input type="checkbox"/> Academics | <input type="checkbox"/> Office of Information Technology |
| <input type="checkbox"/> Auxiliary Services _____ | <input type="checkbox"/> Office of Marketing & Communications |
| <input type="checkbox"/> Business Office _____ | <input type="checkbox"/> Office of Research & Sponsored Programs |
| <input type="checkbox"/> Enrollment Management & Student Success | <input type="checkbox"/> Safety & Security |
| <input type="checkbox"/> Facilities Maintenance & Services | <input type="checkbox"/> Triton Athletics |
| <input type="checkbox"/> Graduate Studies | <input checked="" type="checkbox"/> Other <u>Undergraduate Catalog</u> |
| <input type="checkbox"/> Human Resources Office | |

Location of proposed alteration in manual: Criminal Justice program description **Version dated:** AY 2021-22

- Attach:**
 - Proposed Procedure, Regulation, or Policy language (*in unlocked finalized Word file only, no PDFs*).
 - Documentation showing reason and appropriate consultation with advisory and/or governance committees has been done.
 - Documentation of a public hearing, as applicable.

10. Consultation Record (as per governance guidance, manual, or courtesy)

| Committee | Position | Name / Signature (use BLUE ink) | Date |
|--|-----------------------------------|---------------------------------|---------------------|
| Originating Unit AAC <input type="checkbox"/> NA | See attached curriculum documents | | |
| Appropriate Dean/Director/ Admin <input type="checkbox"/> NA | See attached curriculum documents | | |
| AD HOC Committee <input checked="" type="checkbox"/> NA | _____ | / _____ | _____ / _____ /20__ |
| Student Gov Association <input checked="" type="checkbox"/> NA | _____ | / _____ | _____ / _____ /20__ |
| Staff Council <input checked="" type="checkbox"/> NA | _____ | / _____ | _____ / _____ /20__ |
| Administrative Council <input type="checkbox"/> NA | _____ | / _____ | _____ / _____ /20__ |
| Faculty Senate <input type="checkbox"/> NA | See attached curriculum documents | | |
| Faculty Union <input checked="" type="checkbox"/> NA | _____ | / _____ | _____ / _____ /20__ |

11. Administration Approvals (as applicable)

| | | |
|-----------------------------|-----------------------------------|---|
| Anita Borja Enriquez, SVP&P | See attached curriculum documents | |
| Randy Wiegand, VPAF/CBO | Not applicable | |
| Thomas Krise, UOG President | <u>Thomas W. Krise</u> | <input checked="" type="checkbox"/> Approved <input type="checkbox"/> Disapproved <u>10/23/2020</u> |

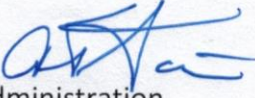
Thomas W. Krise (Oct 23, 2020 08:25 GMT+10)

February 25, 2020

Faculty Office
University of Guam

MEMORANDUM

TO: Dr. Mary Cruz, President
UOG Faculty Senate

FROM: Dr. Annette T. Santos, Dean 
School of Business & Public Administration

SUBJECT: Resubmission and Revision of Proposed Minor in Cybersecurity Management
and Professional Certificate Program in Cybersecurity Management (Reference
Log No. 6147)


Received By:
2/27/20 9:00am
Date & Time

Håfa Adai! Thank you for the opportunity to submit this revised Proposed Minor in Cybersecurity Management and Professional Certificate Program in Cybersecurity Management (Reference Log No. 6147).

The original submission is replaced the attached. This has been vetted and endorsed by the faculty of the Division of Public Administration and Legal Studies during their February 5, 2020 meeting as well as the SBPA-AAC on February 17, 2020 (official Minutes pending).

Should you have any questions or concerns, please contact me at extension 2501/2553 or email: atsantos@triton.uog.edu.

Si Yu'os Ma'åse'.

Attachment

cc: PALS Division Chair
SBPA-AAC Chair
SBPA File

T: +1 671.735.2550 F: +1 671.734.5362 W: www.uog.edu/sbpa

Mailing Address: 303 University Drive UOG Station Mangilao, Guam 96923

The University of Guam is a U.S. Land Grant Institution Accredited by the Western Association of Schools and Colleges Senior College and University Commission and is an Equal Opportunity Employer and Provider.



REQUEST FOR NEW DEGREE PROGRAM APPROVAL

1. Title of Program: MINOR IN CYBERSECURITY MANAGEMENT AND PROFESSIONAL CERTIFICATE IN CYBERSECURITY MANAGEMENT
2. Credit Hours Required: 15
3. Level of Program: Undergraduate Graduate
4. Proposed Effective Date (Catalog/Bulletin): UNDERGRADUATE CATALOG 2020-2021
5. Proposal Document: Attach proposal document to this form. See "Procedure for Proposals to Establish New Programs".
6. APPROVAL Recommended by:



| UNIT | SIGNATURE (use BLUE pen please) | DATE |
|---|---|-------------------|
| For Program | <u>[Signature]</u> | <u>12/10/19</u> |
| Division Chair | <u>Dr. Ronald McNinch, PALS Division Chair</u> | <u>12/10/19</u> |
| Chair, College AAC/CC | <u>[Signature]</u> | <u>2/4/2020</u> |
| Dean, of College | <u>Dr. Annette L. Santos, Dean, SBPA</u> | <u>2/4/2020</u> |
| UCRC/GCRC | <u>Dr. Michael Hemmingsen</u> | <u>5/14/2020</u> |
| President, Faculty Senate (if substantive) | <u>[Signature]</u> (Endorsement of UCRC/GCRC Recommendation) | <u>05/14/2020</u> |

APPROVED:
[Signature]
SENIOR VICE PRESIDENT
ACADEMIC AND STUDENT AFFAIRS

Jun 1, 2020
DATE

[Signature]
Thomas W. Krise
PRESIDENT
10/23/2020
DATE

Jerold W. Filush
CHAIRPERSON, BOARD OF REGENTS
11/24/2020
DATE

Signed via Res 20-36 - 11/24/2020

**PROPOSAL FOR A
MINOR IN CYBERSECURITY MANAGEMENT
AND A
PROFESSIONAL CERTIFICATE PROGRAM
IN
CYBERSECURITY MANAGEMENT**

**SCHOOL OF BUSINESS AND PUBLIC ADMINISTRATION
UNIVERSITY OF GUAM
DECEMBER, 2019**

TABLE OF CONTENTS

PROPOSAL PACKET FOR A MINOR IN CYBERSECURITY MANAGEMENT AND A PROFESSIONAL CERTIFICATE PROGRAM IN CYBERSECURITY MANAGEMENT

- Section 1:** Request For New Degree Program Approval (UOG Form)
Minor in Cybersecurity Management and Professional Certificate Program in
Cybersecurity
- Section 2:** SBPA Proposal for A Minor in Cybersecurity Management and a Professional
Certificate Program in Cybersecurity Management
- Section 3:** Request For New Course(s) (UOG Forms; 5 New Courses)
- Section 4:** Request For New Course Outline(S) (UOG Forms; 5 New Courses)
- Section 5:** Complete CJ-CSM Course Syllabi (5 New Courses)
- Section 6:** Academic and Professional Profiles of Faculty for the Minor in Cybersecurity
Management and Professional Certificate Program in Cybersecurity Management
- Section 7:** Survey Report of Stakeholder Interest and Support for the Minor in Cybersecurity
Management and a Professional Certificate Program in Cybersecurity Management

**Request For New Degree Program
Approval (UOG Form)**

**Minor in Cybersecurity Management
and a
Professional Certificate Program in
Cybersecurity Management**



**REQUEST FOR APPROVAL OF A
NEW MINOR DEGREE AND CERTIFICATE PROGRAM**

1. DEFINITION OF THE PROPOSED PROGRAM

1.1 Full and exact designation (degree, major, minor, certificate, etc.) for the proposed program.

Cyber Security Management Minor and Professional Certificate Program in Cybersecurity Management

1.2 Name of the college submitting the request.

School of Business and Public Administration

1.3 Name of the department, department's division, or other unit of the college which would offer the proposed program.

Division of Public Administration and Legal Studies (PALS)

1.4 Name, title and rank of the individual primarily responsible for the drafting of the proposed program.

Dr. Ronald L. McNinch, Division Chair and Full-Time SBPA faculty in the Public Administration and Legal Studies Program with the participation of PALS and Business faculty.

1.5 Objectives of this program.

The Cybersecurity Management Minor (CJ-CSM) and Professional Certificate Program in Cybersecurity Management are part of an interdisciplinary management approach to cybersecurity in public and private organizations. The primary objectives of this program are to provide students and professionals with the skills and confidence needed to identify problem areas related to cybersecurity and information technology management in an organization and identify solutions. The program is intended to enhance student and participant learning and career opportunities in information security management that can be applied to various organizational settings.

1.5a Specify the subject matter to be covered.

The focus of the course material is on cybersecurity management challenges in an organizational setting. Students will learn about the critical need for protection of data and information, and what to do in the event that protected information is breached. The program is designed to capitalize on the intellectual strengths of students majoring in different disciplines that are consistent with the broad suite



of professional management needs found in varied institutional settings. Students with backgrounds or academic areas of interest in: Criminal Justice, Information Technology, Business, Public Administration, Law, Education, Healthcare, the Behavioral Sciences and many other fields may link their area of interest to this program. The program will cover subject matter in information risk management, computer crime, homeland security, law, defense, terrorism studies, policy development and other topics as they relate to information management and security threats.

- 1.5b Specify the intellectual skills and learning methods to be acquired.

This course of study will provide students with the techniques and tools to deal with cybersecurity management, planning and threats. The methodology of the coursework will provide students and participants with skills to (1) develop an understanding of the importance of cybersecurity management in organizations; (2) identify short and long term cybersecurity threats and problems and their associated consequences for organizations if not properly addressed by management; (3) learn how to gather and analyze relevant information for informed management decision-making and responses to cybersecurity threats; and (4) learn how to think strategically about new ways to approach and solve cybersecurity management challenges in organizations.

- 1.5c Specify the affective and creative capabilities to be developed.

In this program, students will examine cybersecurity and information technology oversight; management techniques and key components in developing cybersecurity plans (see 1.5.b) and search for strategic ways to protect organizations from cybercrimes and intrusions.

- 1.5d Specify, the relevant, the specific career-preparation practices to be mastered.

The 15-credit hour curricula for the proposed Cybersecurity Management Minor and Professional Certificate Program in Cybersecurity Management are designed to provide knowledge in cybersecurity risks and threats in organizations. The program will help students and participants develop confidence in managing cybersecurity challenges in organizations.

- 1.6 List of all courses, by catalog number, title and units of credit to be required for a major under the proposed degree program.

The Minor in Cybersecurity Management (CJ-CSM) and the Professional Certificate Program in Cybersecurity Management would require 15 credit hours of coursework as described below:



- **CJ-CSM 100: Introduction to Cybersecurity Management (3)**
- **CJ-CSM 200: Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks, and the Internet (3)**
- **CJ-CSM 300: Cybersecurity Management Tools and Techniques (3)**
- **CJ-CSM 301: Cybercrime and Digital Forensics (3)**
- **CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives (3)**

1.6a Are there any other upper-division course related to leadership and/or management in this proposed program?

Leadership and Management challenges are emphasized and incorporated in all the five courses designed for this program. (Please see five (5) course syllabi developed for this program in the proposal packet).

1.7 Clarification of number and types of electives, if any under the proposed program, including special options.

A student may petition the Public Administration and Legal Studies Program for consideration to substitute a course they have completed that may be equivalent in content to a course required in the Cybersecurity Management program.

1.8 Justification of any unusual characteristics of the proposed program; e.g., in terminology, units of credit required, types of course work, etc.

No specific “unusual” aspects of the Minor or Certificate program in Cybersecurity Management are apparent in this program.

1.9 Prerequisites and criteria for admission of students to the proposed program, and for their continuation in the program.

The Cybersecurity Management Minor and Certificate Program are open to all current and former University of Guam students and professionals desiring to learn and understand the techniques and tools needed to plan and respond to cybersecurity challenges and threats.

1.10 Evidence the degree program has a coherent design and is characterized by continuity, sequential progression and a synthesis of learning.

The curriculum in the Cybersecurity Management Minor and Certificate program consists of five distinct courses that are presented in sequence. (Please see 1.6) The 100



and 200-level courses provide essential cybersecurity facts and concepts necessary for the understanding and assimilation of the contents of the 300-level courses. The intention of the early courses is not to prepare students for technical careers, but to enhance their skills in understanding and managing information security challenges in a digital world. The 300-level courses address learning relevant to best practices in cybersecurity management, including understanding cybercrime and forensics, planning, administration, policymaking and the law.

1.11 Describe how educational effectiveness of the program is to be measured.

Student Learning Outcome (SLO) assessments will be conducted by performing pre-and-post tests in every class and by developing student learning performance profiles for each class. Hands-on simulation exercise and writing assignments will also be used to measure student performance. The results of these assessments will be used to measure proficiency.

2. CONTEXT OF THE PROPOSED PROGRAM

2.1 Examples of colleges offering the proposed program.

- **University of Virginia: School of Continuing and Professional Studies – Cybersecurity Management Certificate.**
- **St. Thomas University: Gus Machado School of Business -Certificate in Cybersecurity Management.**
- **University of Maryland – University College – Graduate Certificate in Cybersecurity Management.**

2.2 Endorsement from university or community elements.

The faculty and Dean of the UOG School of Business and Public Administration support the proposed Minor and Certificate program in Cybersecurity Management. Input from students, alumni and leaders in public and private organizations on Guam and the region helped in the development of this proposal. A community survey was also conducted to solicit input from students, alumni and public business sector professionals on the proposal. (See Section 7)

2.3 Differences of the proposed program, if any, from similar programs in other institutions.

Academic and certificate programs in Cybersecurity Management are found throughout universities and colleges in the United States and abroad. Some programs are offered at the graduate level while others are offered at the undergraduate level. These programs are usually offered as an area of concentration within a degree program or as a general



curriculum or certificate available to all students. The proposed program at UOG will incorporate a multi-disciplinary approach to cybersecurity management issues and challenges that are particularly relevant to the needs of Guam and the Western Pacific.

- 2.4 Relation of the proposed program to the total educational program of the respective college.

The study of Criminal Justice, Business, Accounting and Public Administration are the largest degree programs at the School of Business and Public Administration. These programs have far reaching implications for the well-being of the public and business sectors of Guam and the regional community. Students enrolled in other UOG schools and Colleges would also benefit from the Management skill sets offered in the Cybersecurity Minor and Certificate Program, particularly topics such as strategic planning and ethical conduct in the cyber world.

- 2.5 Relation of the proposed program to the planned curricular development of the respective instructional area (department, department's division).

The Cybersecurity Management Minor and Certificate Program supplements SBPA offerings and will provide students, alumni and working professionals an opportunity to gain specialized knowledge relevant to their career goals. The Minor will be offered as an option within the Bachelor of Science degree program in Criminal Justice (BSCJ). The Minor will also be available to all University of Guam students. The Certificate Program is intended to serve the needs of working professionals in the Guam and regional community. The program will provide skill sets critically needed in public and private organizations dependent on data information technology and security.

- 2.6 List of other programs currently offered which are closely related to the proposed program.

Various degree programs at the University of Guam currently recommend or require students to complete a course in basic computing. These programs include - SBPA: Business, Criminal Justice, Public Administration, Accounting, Finance, Economics; SOE: Administration and Supervision; Division of Social and Behavioral Sciences: Sociology, Psychology, Social Work, Political Science; Health Sciences: Nursing, etc. These and other degree programs directly relate to careers practiced in organizational environments dependent on information technology and cybersecurity.

- 2.7 Explanation of how the needs to be met by the proposed program have previously been satisfied.



SBPA degree programs have specific classes and/or modules with content in management and administration - however, a focus on cybersecurity management has not been previously developed and offered as a minor and certificate program.

- 2.8 Applicability of course work taken under the proposed program to other programs currently offered.

Students with majors in Criminal Justice, Business, Public Administration, Accounting and other UOG degree programs and professionals in the Guam and regional community will find the Cybersecurity Management Minor and Certificate Program beneficial in enhancing skill sets and career goals.

- 2.9 Assurance that courses and programs are planned both for optimal learning and accessible scheduling and are offered in a manner that ensures students the opportunity to complete the entire program as announced.

The proposed Cybersecurity Management Minor and Certificate Program will be offered during the regular UOG Academic Calendar. The program will also feature an off-campus course delivery option, depending on need. The Cybersecurity Management Program is also designed to be adaptable to both classroom and/or On-line delivery modes.

3. NEED FOR THE PROPOSED PROGRAM

- 3.1 Primary reason for requesting the proposed program.

From the global, national and local challenges facing governments, corporations and organizations with large amounts of data being stored and exchanged electronically, the proposed Cybersecurity Management Minor and Certificate Program will provide students and participants with the skills and confidence needed to make management level decisions in an increasingly complex and technically driven world.

- 3.2 Professional uses of the proposed program.

Organization leaders and managers are becoming more and more aware of the costs associated with maintaining, protecting and securing data and information in the workplace. There is an increased need for managers to be aware of existing cyber threats and who can examine and develop solutions to these threats. With the growing dependence on data stored and shared by organizations, there is a need for knowledgeable managers to address these issues. A Cybersecurity Management Minor and Certificate Program would greatly increase employment opportunities and career advancement for UOG students and program participants.



- 3.3 Results of a survey of serious interest in enrolling under the proposed program.

Interaction of Public Administration and Legal Studies faculty with students, alumni and professionals in public and private organizations on Guam and in the region via a formal survey demonstrates the need for and strong support of the proposed Cybersecurity Management and Certificate Program at the University of Guam. The level of interest from current and former students who participated in the survey has been high.

- 3.4 Enrollment figures during the past two years in specified courses programs related to the proposed which indicates interest in the proposed program.

Because the courses designed for the proposed Cybersecurity Minor and Certificate Program have not been previously offered, no enrollment figures currently exist.

- 3.5 Estimate of the number of students completing the proposed program in the second year and in the fifth year after its approval.

It is estimated that when the Cybersecurity Minor and Certificate Program formally begins at the start of the 2020-2021 Academic Year, between 20-30 students and participants will initially enroll in the program. The start of the program will be preceded by a public information initiative. It is believed almost all program participants will complete the program.

- 3.6 Total FTE lower division and upper division, enrollments in the specified department, department's division, or other units of the college which would offer the proposed program, as of the current semester and as projected five years hence, further divided into lecture FTE and laboratory FTE where appropriate.

This information is not available at this time. Please note, however, that the Cybersecurity Minor and Certificate Program will not require the hiring of new full-time faculty at SBPA. CJ-CSM courses will be covered by current SBPA full-time faculty and adjuncts. Qualified visiting faculty and faculty colleagues from other UOG schools and colleges may also be invited to participate in course delivery.

- 3.7 Advantages to the college offering the proposed program.

The Cybersecurity Management and Certificate Program is designed to give students and participants an understanding of the importance of effective cybersecurity management in public and private organizations. SBPA desires to graduate students who not only know something about a particular academic field, but who can also adapt and apply management principles to new organizational challenges.



4. RESOURCES FOR THE PROPOSED PROGRAM

4.1 List of all present faculty members, with rank, highest degree earned, publications and professional experience, who would teach in the proposed program. Include a schedule of course over the next two years, with an indication of who teaches which course.

- **Dr. Wai K. Law, Ph.D., Professor of Management**
- **Dr. Kevin K.W. Ho, Ph.D., Professor of Management Information Systems**
- **Dr. Ron McNinch, Ph.D., Associate Professor of Public Administration and Legal Studies**
- **Prof. Ron Aguon, JD, Associate Professor of Legal Studies**
- **Dr. John Rivera, Ph.D., Assistant Professor of Public Administration; Graduate Program Director**
- **Prof. Frank Ishizaki, Instructor of Legal Studies, M.S., Ret. FBI Special Agent**

Qualified adjuncts from professional organizations on Guam and visiting professors and faculty colleagues from other schools and colleges at UOG may be invited to assist in the delivery of courses on an as-needed basis.

4.2 Number and types of additional faculty and other staff positions, if any, needed to initiate the proposed program. **NONE**

4.3 Estimate of additional faculty and other staff positions needed specifically for the proposed program one, two and five years after its approval.

Current resources at the School of Business and Public Administration are enough to meet the needs of the Cybersecurity Management Minor and Certificate Program.

4.4 List of courses now offered, by catalog number, title and units of credit needed in proposed program. **NONE**

4.5 List of additional courses not now offered, by catalog number, title and units of credit, needed initially and during the first two years after approval of the program, needed to make the program fully operative.

Approval of the following five (5) new courses (3 credit hours each) are needed to make the Cybersecurity Management Minor and Certificate Program fully operative:

- **CJ-CSM 100: Introduction to Cybersecurity Management**
- **CJ-CSM 200: Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet**
- **CJ-CSM 300: Cybersecurity Management Tools and Techniques**
- **CJ-CSM 301: Cybercrime and Digital Forensics**



- **CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives**

4.6 University library resources, available in direct support of the proposed program, specified by subject areas, volume count, periodical holding, etc.

Current holdings at the University of Guam library and access to relevant periodicals are satisfactory to start up the Cybersecurity Management and Certificate Program. Additional learning material for the program will be available on-line.

4.7 Plans for developing university library resources in support of the proposed program during the first year of its operation.

As new learning resources are identified, requests for acquisition will be made to the University library in support of the Cybersecurity Management Minor and Certificate Program.

4.8 Other instructional materials, if any, needed in support of the proposed program, itemized with cost estimates as projected for the first five years of operating the program.

NONE AT THIS TIME.

4.9 Special classrooms, laboratories and other capital outlay facilities, if any, needed in support of the proposed program, itemized and arranged by dates for the first five years of operating the program.

SBPA has two computer labs and sufficient classrooms available to support the Cybersecurity Management Minor and Certificate Program. The faculty who will participate in course delivery have IT equipment available to them in their offices and in the classrooms. SBPA also has a full-time IT specialist on staff available to assist faculty and students.

SBPA PROPOSAL:

Minor in Cybersecurity Management and a Professional Certificate Program in Cybersecurity Management

**PROPOSAL FOR A
MINOR IN CYBERSECURITY MANAGEMENT
AND A
PROFESSIONAL CERTIFICATE PROGRAM
IN
CYBERSECURITY MANAGEMENT
School of Business and Public Administration
UNIVERSITY OF GUAM**

INTRODUCTION

Cybersecurity Management (CSM) is a growing field of study in the United States and abroad, generally covering topics in information risk management related to computer crime, homeland security, terrorism studies, policy development, and related areas. Information security threats are growing in intensity, frequency, and severity all over the world, and are also a very real threat to the information security of public and business organizations on Guam and in the Western Pacific.

The School of Business and Public Administration, University of Guam, is proposing a course of study in Cybersecurity Management (CSM) both as a Minor within the Bachelor of Science in Criminal Justice degree program (BSCJ) which will be available to all University of Guam students, and as a Professional Certificate Program for alumnae and professionals in the public and private sector. The courses shall use the "CJ-CSM" identifier for course listing purposes.

This program is not intended to be a technical course of study. The information systems and cybersecurity management principles incorporated in this proposal are designed to capitalize on the intellectual strengths of students majoring in different disciplines at UOG that are consistent with the broad suite of professional management needs found in varied institutional settings on Guam and in the region.

In preparing this proposal, it was found that most academic programs in information security are technical in nature, usually offered through computer science or computer engineering departments at colleges and universities. Their intent is to produce information professionals who are primarily developers; (e.g., software engineers, system administrators, and network administrators). Criminal Justice degree and certificate programs have largely arisen as applied management curricula. This is the case of the BSCJ program at the University of Guam.

The approach that will be taken with the proposed Cybersecurity Management Minor and Certificate Program is to respond to the evolving cyberthreats facing Guam and the region that are not solely based on technical solutions. This will involve planning and information security topics as applied to economics, business, public administration, criminal justice,

finance, homeland security, diplomacy, national defense and other areas. The proposed skill set will provide a management context to the program and will emphasize those management principles, tools and concepts required of professionals charged with effectively overseeing or managing public and private information infrastructure critical to Guam and the region.

In this program students and participants will learn to employ and understand technology tools to plan for and solve cybersecurity problems in organizations. These skill sets are critically needed in government and business institutions to support the day-to-day functioning of the information security management tasks.

The management of the cybersecurity function includes the development of internal policies and procedures as well as laws and public policy. SBPA will use a proactive, defensive and offensive management approach in program delivery that will teach students to be able to respond to a cybersecurity event, and design and execute necessary actions in order to defend, protect or effectuate a response to a cybersecurity attack. The program does not force students into an engineering-based approach to cybersecurity. Rather, the program will integrate the National Response Framework of the U.S. Department of Homeland Security into a curriculum that will fully explore intelligence gathering, threat analysis, planning, management, policy development, risk analysis and mitigation. These are the subjects taught in the SBPA Criminal Justice program that are not generally taught in traditional computer engineering programs.

In this program, students will not need engineering or information technology expertise in order to understand and learn how to lead and manage a response to the threats in cyberspace. But they will need cyber-literacy, which will be integrated into the program curricula in order to understand a threat issue and synthesize the ramifications with the I.T team into other aspects of security. The program will not require students to take additional courses in mathematics but will require the ability of students to manipulate numbers and symbols and be comfortable with computer technology. Problem-solving and strategic thinking and planning skills are also important.

PROPOSED CURRICULA/COURSES

Exploration and input from students, stakeholders in business and government, external advisors, and a review of curricula offered by other institutions helped in the development of this proposal to integrate Cybersecurity Management (CJ-CSM) into the BSCJ curriculum as a minor and certificate program. Included in the 15-credit hour Minor and Certificate Program is an introductory cybersecurity course (3 credit hours) to be integrated into the CJ core as a Lower Division elective that shall be available to interested UOG students. There are four other courses developed as part of the Minor and Certificate program, which can be taken by any UOG student, alumnae or stakeholder.

The five courses (15-credit hours) and their general sequencing are shown below. Their content and role in the overall curriculum are also described:

1. **CJ-CSM 100: INTRODUCTION TO CYBERSECURITY MANAGEMENT.** This will be introduced as a lower division elective course for all interested UOG students and as one of the required courses for students and others pursuing the Cybersecurity Management Minor or Certificate Program. The course is a survey of the subject matter, addressing cybersecurity management operations, governance, applications, purposes, and strengths and limitations to information assurance and incident response activities. Topics include a definition of cybersecurity and information security, the need for management training in this field of study, ethical and legal issues, risk management and planning in public and business organizations, and cybersecurity and information security technology. The role of Federal agencies (e.g. Department of Homeland Security, Department of Defense, National Security Council, CIA, FBI, etc.) in securing cyberspace and the nation's information-related infrastructure will be explored. The information security capabilities of local agencies and institutions will also be discussed. A goal of this class will be to apply the topics discussed in the assessment of security risks in the protection and management of information assets in both public and private organizations.

The remaining four courses are also part of the Cybersecurity Management Minor and Certificate Program. In these courses, students and program participants will not need to be computer programmers or network experts to learn cybersecurity management applications. However, they should have some experience in the use of technology. Some of these courses may be offered on-line by SBPA or via a cooperating academic institution.

2. **CJ-CSM 200: FUNDAMENTALS OF COMPUTERS AND NETWORKING TECHNOLOGIES FOR CYBERSECURITY MANAGERS IN ORGANIZATIONS: UNDERSTANDING COMPUTER HARDWARE, NETWORKS, AND THE INTERNET.** This class is intended to provide an introduction to the technology that underlies computers and communication networks. Students will gain an understanding of how computers operate, user interfaces and operating systems, data storage, network hardware components and protocols, Internet and Transmission Control Protocols (TCP/IP), communications protocols and applications. This course is not intended as a security management course per se, but as one that covers the fundamental bases of the technologies that students, organizations, and managers use every day in organizational life and that are, in fact, the vectors of cyberattacks. The course is heavily dependent upon hands-on exercises to reinforce the course subject matter, (e.g., exercises are planned that will introduce both the DOS and Linux command line interface, students will build peer-to-peer networks, write a simple program, install a simple Web server, write a Web page, utilize a firewall, and identify cyberattack intrusions). The intent of the exercises is not to turn managers of business and government organizations into system administrators, Web designers, or programmers, but to help these managers understand and appreciate what IT professionals do, how the systems they use operate, and how they can assist and lead them in a cyber threat incident and recovery situation.

The above 100 and 200-level courses are the prerequisites for the remaining 300-level courses:

3. **CJ-CSM 300: CYBERSECURITY MANAGEMENT TOOLS AND TECHNIQUES.** This course is intended to introduce the tools and techniques used to attack and disrupt computers, data networks, and digital information; demonstrate methods by which attackers identify and exploit organization vulnerabilities and weaknesses in information systems. The course will introduce and demonstrate risk management techniques and methods and demonstrate how to secure operating systems, communications infrastructure, and data networks including TCP/IP and the Internet. The basics of planning and conducting security audits and developing cybersecurity policies in organizations will be studied.
4. **CJ-CSM 301: CYBERCRIME AND DIGITAL FORENSICS.** This second 300-level course is a hands-on and focuses on the tools and techniques of reactive offense and defense in cybersecurity management. Recent trends in Mobile and Digital forensics, Block Chain forensics, and Cryptocurrency and Cloud Computing forensics will be discussed. The course will introduce the practices of incident response, and digital investigations, penetration testing and vulnerability assessments, and the gathering of digital information for evidentiary, intelligence, and research purposes. Legal aspects governing criminal justice search and seizure will be described, as well as the basic tools for computer, network, and mobile device forensics acquisition, analysis, and reporting.
5. **CJ-CSM 302: LEGAL ISSUES AND CASES IN CYBERSECURITY AND THE LAW: LOCAL, NATIONAL, AND INTERNATIONAL PERSPECTIVES.** This course will address criminal behavior in cyberspace, such as identity theft, white-collar crime, fraud, child sexual exploitation, human trafficking, intellectual property theft, and on-line scams. Evolving laws governing cyberspace, defining criminal activity, and guiding law enforcement investigations will be covered, including U.S. decisional law that guide the search and seizure of digital devices and information as well as international and local laws related to cybercrime and privacy that challenge public and private organizations. The course will examine the impact of cyberspace, cybercrime and espionage on government and business institutions, diplomacy, defense and terrorism, including emergent threats and modern countermeasures, and how critical infrastructure can be hardened and made more resilient in order to reduce the potential impact of cyberattacks. This legal approach to cybersecurity management is particularly important and timely for business and government organizations as the United States has experienced many cases of cyberterrorism and cyberwarfare, as evidenced by "Advanced Persistent Threat" attacks on U.S. information hardware and information systems for political and ideological goals. Cyberattacks on social networks, American-owned financial and banking institutions, electric power grids, and diplomatic and defense communication intrusions are now common.

ASSESSMENT INSTRUMENTS

In the Cybersecurity Management and Certificate Program, the 100 and 200-level courses will provide essential cybersecurity facts and concepts necessary for the understanding and assimilation of the contents of the 300-level courses. Since the intention of the early courses is not to prepare students for technical careers or jobs - but rather to enhance their skills in understanding and managing information security in the digital world - the testing will not focus on the technical aspects of the subject matter. Instead, assessment mechanisms will be prepared that better measure what students and certificate participants have learned about technology management and will address the learning outcomes of the courses that are relevant to best practices in security policy, administration, and management. Hands-on exercises and writing assignments will be used to measure whether students have achieved defined learning outcomes rather than traditional objective assessment tests.

CONCLUDING POINTS

The Criminal Justice program at the School of Business and Public Administration, University of Guam, has grown to be a robust, dynamic, and valuable academic offering to students and stakeholders. As new needs arise, this program continually matures and adapts. The proposed Cybersecurity Management (CJ-CSM) Minor and Certificate Program is part of this evolution. This new program will provide students and participants with a valuable and critical management skill set to be able to address one of the most challenging issues facing public and private organizations today - Cybersecurity.

The Cybersecurity Management Minor and Certificate Program will require the participation of SBPA faculty with subject matter expertise and the use of identified cybersecurity management professionals in local public and business organizations which will help broaden the learning opportunities and outcomes for students and program participants. Faculty colleagues from other units of the University of Guam may also be invited to participate in program delivery.

**CYBER SECURITY MANAGEMENT (CSM) MINOR
AND
PROFESSIONAL CERTIFICATE PROGRAM
IN
CYBERSECURITY MANAGEMENT**

Bibliography/References Used in Preparing Program Proposal

Abawajy, J., 'User preference of cyber security awareness delivery methods, Behaviour and information technology', Vol. 33, No 3, 2014, pp. 237-248.

Albrechtsen, E., & Hovden, J., 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An Intervention Study', Computer and Security, Vol. 29, No 4, pp. 432-445.

Alfawaz, S., Nelson, K., Mohannak, K., 'Information security culture: A Behaviour Compliance Conceptual Framework', 8th Australasian Information Security Conference, Brisbane, Australia, 2010.

Alnatheer, M., 'A Conceptual Model to Understand Information Security Culture', Int. J. Soc. Sci. Humanit., Vol. 4, No 2, 2014, pp. 104-107.

Alnatheer, M., Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia, 2012.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L., 'Gender difference and employees' cybersecurity behaviors', Computers in Human Behavior, 2017.

Ardichvili, A., Page, V., & Wentling, T., 'Motivation and barriers to participation in virtual knowledge-sharing communities of practice', Journal of Knowledge Management, Vol. 7, No 1, 2003.

Argyris, C., & Schön, D., Organizational learning, Addison-Wesley, Reading, 1978.

Asch, S., 'Studies of independence and conformity: A minority of one against a unanimous majority', Psychological monographs: General and applied, Vol. 70, No 9, 1956, pp. 1-70.

Ashenden, D., 'Information Security management: A human challenge?' Information Security Technology Report, Vol. 13, No 4, 2008, pp. 195-201.

Ashenden, D., & Sasse, A., 'CISOs and Organisational Change: Their Own Worst Enemy?', Computers & Security, Elsevier, 2013.

Atom, I., Otoom, A., & Ali, A., 'A holistic cyber security implementation framework', Information Management & Computer Security, Vol. 22, No 3, 2014, pp. 251-264.

Australian Department of Defence, Human Factors and Information Security, no date.

Beautement, A., Sasse, A., & Wonham, M., The Compliance Budget: Managing Security Behaviour in Organisations, 2008.

Business Software Alliance, Information Security Governance, 2013.

Cheng, Y., Li, W., Holm, E., & Zhai, Q., 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory', Computer Security, Vol. 39, 2013, pp. 447-459.

Chipperfield, C., & Furnell, S., 'From security policy to practice: Sending the right messages', Computer Fraud Security, Vol. 2010, No 3, 2010, pp. 13-19.

CISCO, Cybersecurity Management Program, 2017.

Cook, S., & Yanow, D., 'Culture and organizational learning'. *Journal of Management Inquiry*, Vol. 2, No 4, 1993, pp. 373-390.

D'Arcy, J., Hovav, A., & Galletta, D., 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach', *Information Systems Research*, Vol. 20, No 1, 2009, pp. 79-98.

Das, S., Kim, T., Dabbish, L., & Hong, J., The Effect of Social Influence on Security Sensitivity, Symposium on Usable Privacy and Security (SOUPS), Menlo Park 2014.

Da Veiga, Information Security Culture Assessments, 2014.

Deal, T., & Kennedy, A., *Corporate cultures*, Addison-Wesley, Reading, 1982.

Deal, T., & Kennedy, A., *The new corporate cultures*, Perseus, New York, 1999.

Denison, D., *Corporate Culture and Organizational Effectiveness*, Wiley, New York, 1990.

Deloitte, Risk Intelligent governance in the age of cyber threats, 2012.

Detert, J., Schroeder, R., & Mauriel, J., 'A Framework for Linking Culture and Improvement Initiatives in Organisations'. *Academy of Management Review*, Vol. 25, No 4, 2000, pp. 850-863.

Dimensional Research, Trends in Security Framework Adoption, 2016.

Dodge, R., Carver, C., & Ferguson, A.J., 'Phishing for User Security Awareness', *Computers and Security*, Vol. 26, 2007, pp. 73-80.

Dojkovski, S., Lichtenstein, S., & Warren, M., Fostering information security culture in small and medium size enterprises: an interpretive study in Australia, in *Proceedings of the 15th European Conference on Information Systems*, University of St. Gallen, St. Gallen, 2007, pp. 1560-1571.

Earnst & Young, Cyber Program Management, 2014.

Eminagaoglu, M., Ucar, E., & Eren, S., 'The positive outcomes of information security awareness training in companies – a case study'. *Information Security Technical Report*, Vol. 4, 2010, pp. 1-7.

ENISA, Measurement Framework and Metrics for Resilient Networks and Services: Challenges and recommendations, 2011.

ENISA, Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures, 2016.

Fagerström, A., *Creating, Maintaining and Managing an Information Security Culture*, 2013.

Fitzgerald, T., Building Management Commitment through Security Councils, or Security Council Critical Success Factors, In H. F. Tipton (Ed.), *Information Security Management Handbook*, Auerbach Publications, Hoboken, 2007, pp. 105-121.

Foley & Lardner LLP, Taking Control of Cybersecurity, 2015.

Furnell, S., *A Conceptual Model for Cultivating an Information Security Culture*, 2015.

- Furnell, S., & Clarke, N., *Organisational Security Culture: Embedding Security Awareness, Education and Training*, 2005.
- Furnell, S., & Thomson, K., 'From culture to disobedience: Recognising the varying user acceptance of IT security', *Computer Fraud Security*, Vol. 2009, No 2, 1999, pp. 5-10.
- Geertz, C., *The interpretation of cultures*, Basic Books, New York, 1973.
- Goffman, E., *The presentation of self in everyday life*, Doubleday, New York, 1959.
- Goffman, E., *Interaction ritual*, Hawthorne, Aldine, 1967.
- Greene, G., & Arcy, J., 'Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance', 2010, pp. 1-8.
- Halevi, T., et al., 'Cultural and Psychological Factors in Cyber-Security', iiWAS '16, November, 2016.
- Hearth, T., & Rao., 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, Vol. 47, No 2, 2009a, pp. 154-165.
- Hearth, T., & Rao, H., 'Protection motivation and deterrence: a framework for security policy compliance in organizations', *European Journal of Information Systems*, Vol. 18, No 2, 2009b, pp. 106-125.
- Henderson, R., & Clark, K., 'Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms'. *Administrative Science Quarterly*, Vol. 35, 1990, pp. 9-30.
- Herley, C., 'More is not the answer', *IEEE Security & Privacy*, Vol. 12, No 1, 2014, pp. 14-19.
- Hewlett Packard, *Awareness is only the first step*, 2015.
- Homans, G., *The human group*, Harcourt Brace Jovanovich, New York, 1950.
- Hong, J., Das, S., Kim, T., Dabbish, L., *Social Cybersecurity: Applying Social Psychology to Cybersecurity*, Human Computer Interaction Institute, Carnegie Mellon University, 2015.
- IBM, *X-Force Threat Intelligence Index*, 2017.
- ISC, *Global Information Security Workforce Study*, 2015.
- Ifinedo, P. 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory'. *Computers & Security*, Vol. 31, No 1, 2012, pp. 83-95.
- Jones, M., Moore, M., & Snyder, R., (Eds.) *Inside organizations*, Sage, Thousand Oaks, 1988.
- Karahanna, E., Straub, D., Chervany, N., 'Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs', *MIS Quarterly*, Vol. 23, No 2, 1999.
- Kilmann, R., & Saxton, M., *The Kilmann-Saxton culture gap survey*. Organizational Design Consultants, Pittsburgh, 1983.
- Koh, K., Ruighaver, A., Maynard, S., & Ahrnad, A, *Security Governance: Its impact on Security Culture*, 3rd Australian Information Security Management Conference, Perth, 2005.

Kruger, H., & Kearney, W., 'A prototype for assessing information security awareness'. *Computers & Security*, Vol. 25, No 4, 2006, pp. 289 – 296.

Lacey, D., *Managing the Human Factor in Information Security: How to win over staff and influence business managers*, Wiley, 2009a.

Lacey, D., 'Understanding and Transforming Organisational Culture', *Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance*, 2009b.

Leidner, D., & Kayworth, T., 'A review of culture in information systems research: towards a theory of information technology culture conflict', *MIS Quarterly*, Vol. 30, No 2, 2006, pp. 357-399.

Lim, J., Chang, S., Maynard, S., & Ahmad, A., Exploring the Relationship between Organizational Culture and Information Systems Security Culture, in *Proceedings of the 7th Australian Information Security Management Conference*, Edith Cowan University, 2009, pp. 87-97.

Malandrin, L., & Carvalho, T., 'Maintaining Information Security in the New Technological Scenario', Vol. 5, No 3, 2013.

Martins, A., & Eloff, J., *Information Security Culture*, 2002, p. 204-206.

Maynard, S., *Exploring Organisational Security Culture – Research Model*, 2002.

Maynard, S., & Ruighaver, A., *Evaluating IS Security Policy Development*, 2002.

McBride, M., Carter, L., & Warkentin, M., *The Role of Situational Factors and Personality on Cybersecurity Policy Violation*, Institute for Homeland Security Solutions, 2012.

McKinsey, *Meeting the Cybersecurity Challenge*, 2011.

Ministry of Finance of Finland, *Effective Information Security*, 2009.

Morris, M., Venkatesh, V., & Ackerman, P., 'Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior'. *IEEE Transactions on Engineering Management*, Vol. 52, No 1, 2005, pp. 69-84.

Ngo, L., *IT Security Culture Transition Process*, 2008.

Niekerk, J. Van., & Solms, R. Von., *An holistic framework for the fostering of an information security sub-culture in organizations*. *Information Security South Africa (ISSA)*, 2005.

Nosworthy, J., *Implementing information security in the 21st century - do you have the balancing factors?*, 2000.

OECD, *Digital Security Risk Management for Economic and Social prosperity*, 2015.

O'Neill, B., *Developing a Risk Communication Model to Encourage Community Safety from Natural Hazards*, *Fourth NSW Safe Communities Symposium*, Sydney, 2004

Pahnila, S., Siponen, M., & Mahmood, A., *Employees' behavior towards IS security policy compliance*, Hawaii, 2007.

PCI Security Standards Council, *Best Practices for Implementing a Security Awareness Program*, 2014.

- Peters, T., & Waterman, R., *In search of excellence*, HarperCollins, New York, 1982.
- Ponemon Institute, *The human factor in data protection* [online], 2012.
- Ponemon Institute, *Cost of Cyber Crime Study and the Risk of Business Innovation*, 2016.
- Ponemon Institute, *Cost of Data Breach Study*, 2016.
- Ponemon Institute, *Cost of Data Breach Study*, 2017.
- Post, G., & Kagan, A., 'Evaluating information security trade-offs: restricting access can interfere with user tasks', *Computers & Security*, Vol. 26, No 3, 2007.
- Ramachandran, S., Srinivasan, V., & Goles, T., 'Information Security Cultures of Four Professions: A Comparative Study'. Paper presented at the 41st Hawaii International Conference on System, Hawaii, 2004.
- RAND, *Cybersecurity economic issues*, 2008.
- Reid, R., & Van Niekerk, J., 'A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory', *HAISA*, 2015, pp. 34-44.
- Robbins, S., *Organizational Behavior: Concepts, Controversies, and Applications (Fourth Edition ed.)*, Prentice Hall, New Jersey, 1989.
- Roer, K., *How to build and maintain security culture*, 2014.
- Roer, K., & Petrič, G., *CLTRe Indepth insights into the human factor: The 2017 Security Culture Report*, 2017.
- Ross, S., & Masters, R., *Creating a Culture of Security*, 2011.
- Rowe, D., Lunt, B., & Ekstron, J., *The Role of Cyber-Security in Information Technology Education*, 2011.
- RSA, *Translating Security Leadership into Board Value*, 2017.
- Sasse, A., 'Scaring and bullying people into security won't work', *IEEE Security & Privacy*, Vol. 3, 2015, pp. 80-83.
- Sasse, A., & Smith, M., 'The Security-Usability Tradeoff Myth', *IEEE Security & Privacy*, Vol. 14, No 5, 2016, pp. 11-13.
- Schein, E., *Coming to a New Awareness of Organizational Culture*, 1984, pp. 2-3.
- Schein, E., *Organizational Culture and Leadership*, Jossey-Bass, San Francisco, 1992.
- Schein, E., 'Empowerment, coercive persuasion and organizational learning: do they connect?', *The Learning Organization*, Vol. 6, No 4, 1999, pp. 163-172.
- Schein, E., *Organizational Culture and Leadership*, 2004, p. 334.
- Schlienger, T., *Tool Supported Management of Information Security Culture*, 2005.
- Schlienger, T., & Teufel, S., *Information Security Culture - the Social-Cultural Dimension in Information Security Management*, 2002.

- Siponen, M., & Willison, R., 'Information security management standards: Problems and solutions', *Information & Management*, Vol. 46, No 5, 2009, pp. 267-270.
- Smircich, L., 'Concepts of culture and organizational analysis'. *Administrative Science Quarterly*, Vol. 28, 1983, pp. 339-358.
- Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J., 'Analysis of end user security behaviors', *Computers & Security*, Vol. 24, No 2, 2005.
- Susanto, H., Almunawar, M., & Tuan, Y., 'Information security management system standards: A comparative study of the big five', *International Journal of Electrical Computer Sciences*, Vol. 11, No 5, 2011, pp. 23-29.
- Symantec, Internet Security Threat Report, 2017.
- Tarimo, C., ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach, 2006.
- Thomson, K., & von Solms, R., 'Information security obedience: a definition', *Computer Security*, Vol. 24, No 1, 2005, pp. 69-75.
- Thomson, K., von Solms, R., & Louw, L., 'Cultivating an organizational information security culture', *Computer Fraud Security*, October, 2006, pp. 49-50.
- Thompson, R., Higgins, C., Howell, J., 'Influence of experience on personal computer utilization', *Journal of Management Information Systems*, Vol. 11, No 1, 1994.
- Trice, H., & Beyer, J., Using six organizational rites to change culture, Jossey-Bass, San Francisco, 1985, pp. 370-399.
- Trice, H., & Beyer, J., *The cultures of work organizations*, Prentice Hall, Englewood Cliffs, 1993.
- Van den Steen, E., *On the Origin of Shared Beliefs (and Corporate Culture)*, MIT School of Management, 2005.
- Van Niekerk, J., 'Establishing an information security culture in organizations: an outcomes based education approach', PhD diss., Nelson Mandela Metropolitan University, 2005.
- Van Niekerk, J., *A Holistic Framework for Fostering IS sub-culture in organizations: an outcomes based education approach*, 2005.
- Van Niekerk, J., & von Solms, R., *An Holistic Framework for the Fostering of an Information Security Sub-Culture in Organizations*, Centre for Information Security Studies, Nelson Mandela Metropolitan University, 2005.
- Venkatesh, V., Morris, M., Davis, G., & Davis, F., 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, Vol. 27, No 3, 2003.
- Verizon, Data Breach Investigations Report, 2016.
- Von Solms, B., 'Information Security -- the Third Wave?', *Computers & Security*, Vol. 19, No 7, 2000, pp. 615-620.

Von Solms, R., 'Information security management: why standards are important', *Information Management & Computer Security*, Vol. 7, No 1,1999, pp. 50-58.

Vroom, R., & von Solms, R., 'Towards information security behavioural compliance', *Computer Security*, vol. 23, no. 3, 2004, pp. 191-198.

Wasko, M., Faraj, S., 'It is what one does: why people participate and help others in electronic communities of practice', *Journal of Strategic Information Systems*, Vol. 9, 2000.

Weick, K., *Sensemaking in organizations*, Sage, Thousand Oaks, 1995.

World Economic Forum, *A Framework for Assessing Cybersecurity Resilience*, 2016.

Yanus, S., & Shin, R., *Critical Success Factors for Managing an Information Security Awareness Programme*, 2007.

REQUEST FOR NEW COURSE(S)

(UOG Form)

- **CJ-CSM 100:** Introduction to Cybersecurity Management
- **CJ-CSM 200:** Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet
- **CJ-CSM 300:** Cybersecurity Management Tools and Techniques
- **CJ-CSM 301:** Cybercrime and Digital Forensics
- **CJ-CSM 302:** Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives



REQUEST FOR NEW COURSE

- 1. Title: Introduction To Cybersecurity Management
- 2. Catalog Number: ^{PC}~~CJ~~-CSM 100 (New course may not duplicate active or inactive course number.)
- 3. Course Type: Addition to the Curriculum
 Special Needs (Workshop, seminar, special topic,...94 series, etc.)
- 4. Level of Instruction: Undergraduate Graduate (/G) Both
- 5. Credit Hours: 3.00
- 6. Is this course cross-listed with another department? NO
 If so, list the cross-listed catalog number (s)? _____
- 7. What session(s) will the course be offered? Fall Spring Summer All
- 8. What will be the yearly cycle for this course?
 All Years Even Years Odd Years One (1) Term Only
- 9. First term and year for this course: Fall 2020-2021 Length of Instruction (Weeks): 16 Weeks
- 10. Prerequisites:
 - A. Instructor / Advisor consent required? Yes No
 - B. Prerequisites Catalog # Prerequisite Course Title
 NONE NONE

 - C. Additional Prerequisites: NONE



11. **CATALOG DESCRIPTION:** This course introduces students to the growing legal, technical, managerial, economic and social issues surrounding crimes committed in cyberspace. The course discusses the nature of cybercrime from a management and international perspective and focuses on how the borderless nature of cybercrime impacts law enforcement and cybersecurity in public and business organizations.
12. **DESCRIBE LIBRARY AND INFORMATION TECHNOLOGY RESOURCES AVAILABLE TO SUPPORT COURSE:** If insufficient library sources are available, describe alternatives that will be used.
Current learning resource holdings at the UOG-RFK Library and access to relevant periodicals are satisfactory to start up this course. Additional course-related material is available on-line. A course website will be designed by the instructor for this course that will be available to students upon enrollment. Additional resources will be available on the course Website, as well as, links to course-related material.
13. **SUBSTANTIATE THE COMPELLING NEED FOR THE NEW COURSE:** **Organization leaders in business and government are becoming more aware of the risks and costs associated with managing, securing and protecting data and information in the workplace. In modern organizations - dependent on information technology, managers need to be aware of cyber threats and be able to develop plans and solutions to deal with these threats. With the growing dependence on data stored and shared by organizations, managers need to be knowledgeable about cybersecurity tools and techniques to address these issues. The knowledge learned in this course will help enhance the job opportunities and career advancement of students.**
14. **WHAT IS THE ANTICIPATED CLASS SIZE AND DOCUMENT INDICATIONS ON HOW THE NEW COURSE WILL MEET ITS PROJECTED SIZE.** **It is estimated that between 20-30 students and Cybersecurity Certificate participants will initially enroll in this course based on discussions and a survey with students, alumni and potential participants from government and business organizations on Guam and in the region. A public information initiative directed at UOG students and business and government organizations will precede the offering of this course and other new cybersecurity management courses prior to the start of the Fall Semester 2020-2021.**
15. **STATE HOW THE NEW COURSE WILL BE COVERED BY EXISTING PROGRAM FACULTY.** **The School of Business and Public Administration has excellent faculty resources to support this new course and other courses in the CJ-CSM Minor and Certificate program. Qualified Adjuncts from professional business and government organizations on Guam, as well as, visiting Professors and faculty colleagues from sister colleges and schools at UOG may be invited to participate in course delivery on an as-needed basis. SBPA has Full-Time and Adjunct faculty resources adept in information technology, forensics, law enforcement and policy-making who desire to participate in course delivery.**
16. **ADDITIONAL INFORMATION:** **Please refer to the “Cybersecurity Management and Professional Certificate Program in Cybersecurity Management Proposal” document and Course Syllabi.**
17. **ATTACH COURSE OUTLINE:** **Please see attached Course Outline. Also refer to the CJ-CSM 100 Syllabus submitted with the proposal packet.**



UNIVERSITY OF GUAM
Unibetsedåt Guåhan

Office of Academic and Student Affairs

APPROVAL RECOMMENDED BY:

| UNIT | SIGNATURE (use BLUE pen please) | DATE |
|---|---|------------|
| For Program | | 12/1/99 |
| Administrative Chair | | 12/1/99 |
| Chair, College AAQ CC | | 7/4/2020 |
| Dean, of College | Dr. Annette F. Santos, Dean, SBPA | 2/4/2020 |
| UCRC/GCRC | Dr. Michael Hemmingsen | 5/14/2020 |
| President, Faculty Senate (if substantive) | (Endorsement of UCRC/GCRC Recommendation) | 05/14/2020 |

APPROVED:

ANITA GORJA ENRIQUEZ (Jun 1, 2020 20:49 GMT+10)
SENIOR VICE PRESIDENT
ACADEMIC & STUDENT AFFAIRS

Jun 1, 2020
DATE



REQUEST FOR NEW COURSE

1. Title: **Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet** _____.
2. Catalog Number: ^{SC} ~~CJ~~-CSM 200 _____ (New course may not duplicate active or inactive course number.)
3. Course Type: Addition to the Curriculum
 Special Needs (Workshop, seminar, special topic,...94 series, etc.)
4. Level of Instruction: Undergraduate Graduate (/G) Both
5. Credit Hours: 3.00 _____
6. Is this course cross-listed with another department? NO _____
 If so, list the cross-listed catalog number (s)? _____
7. What session(s) will the course be offered? Fall Spring Summer All
8. What will be the yearly cycle for this course?
 All Years Even Years Odd Years One (1) Term Only
9. First term and year for this course: Fall 2020-2021 Length of Instruction (Weeks): 16 Weeks
10. Prerequisites:
 - A. Instructor / Advisor consent required? Yes No
 - B. Prerequisites Catalog # Prerequisite Course Title
 NONE NONE

 - C. Additional Prerequisites: NONE



11. **CATALOG DESCRIPTION:** This course introduces students to the growing legal, technical, managerial, economical and social issues surrounding crimes committed in cyberspace. The course discusses the nature of cybercrime from a management and international perspective and focuses on how the borderless nature of cybercrime impacts law enforcement and cybersecurity in public and business organizations.
12. **DESCRIBE LIBRARY AND INFORMATION TECHNOLOGY RESOURCES AVAILABLE TO SUPPORT COURSE:** If insufficient library sources are available, describe alternatives that will be used.
Current learning resource holdings at the UOG-RFK Library and access to relevant periodicals are satisfactory to start up this course. Additional course-related material is available on-line. A course website will be designed by the instructor for this course that will be available to students upon enrollment. Additional resources will be available on the course Website, as well as, links to course-related material.
13. **SUBSTANTIATE THE COMPELLING NEED FOR THE NEW COURSE:** **Organization leaders in business and government becoming more aware of the risks and costs associated with managing, securing and protecting data and information in the workplace. In modern organizations - dependent on information technology, managers need to be aware of cyber threats and be able to develop plans and solutions to deal with these threats. With the growing dependence on data stored and shared by organizations, managers need to be knowledgeable about cybersecurity tools and techniques to address these issues. The knowledge learned in this class will help enhance the job opportunities and career advancement of students.**
14. **WHAT IS THE ANTICIPATED CLASS SIZE AND DOCUMENT INDICATIONS ON HOW THE NEW COURSE WILL MEET ITS PROJECTED SIZE.** It is estimated that between 20-30 students and Cybersecurity Certificate participants will initially enroll in this course based on discussions with students, alumni and potential participants from government and business organizations on Guam and in the region. A public information initiative directed at UOG students and business and government organizations will precede the offering of this course and other new cybersecurity management courses prior to the start of the Fall Semester 2020-2021.
15. **STATE HOW THE NEW COURSE WILL BE COVERED BY EXISTING PROGRAM FACULTY.** The School of Business and Public Administration has excellent faculty resources to support this new course and other courses in the CJ-CSM Minor and Certificate program. Qualified Adjuncts from professional business and government organizations on Guam, as well as, visiting Professors and faculty colleagues from sister colleges and schools at UOG may be invited to participate on an as-needed basis. SBPA has Full-Time and Adjunct faculty resources adept in information technology, forensics, law enforcement, policy-making and the law who desire to participate in course delivery.
16. **ADDITIONAL INFORMATION:** Please refer to the "Cybersecurity Management and Professional Certificate Program in Cybersecurity Management Proposal" document and Course Syllabi.


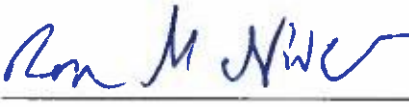



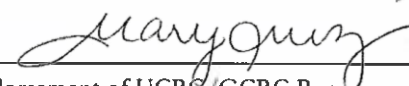


UNIVERSITY OF GUAM
Unibetsedåt Guåhan

Office of Academic and Student Affairs

17. ATTACH COURSE OUTLINE: Please see attached Course Outline. Also refer to the CJ-CSM 100 Syllabus submitted with the proposal packet.

APPROVAL RECOMMENDED BY:

| UNIT | SIGNATURE (use BLUE pen please) | DATE |
|---|---|------------|
| For Program |  | 12/10/19 |
| Administrative Chair |  | 12/10/19 |
| Chair, College AAC/CC |  | 2/4/2020 |
| Dean, of College |  Dr. Annette T. Santos, Dean, SBPA | 2/4/2020 |
| UCRC/GCRC | Dr. Michael Hemmingsen  | 5/14/2020 |
| President, Faculty Senate (if substantive) |  (Endorsement of UCRC/GCRC Recommendation) | 05/14/2020 |

APPROVED:


SENIOR VICE PRESIDENT
ACADEMIC & STUDENT AFFAIRS

Jun 1, 2020
DATE



REQUEST FOR NEW COURSE

1. Title: Cybersecurity Management Tools and Techniques
2. Catalog Number: ²²~~CJ~~-CSM 300 (New course may not duplicate active or inactive course number.)
3. Course Type: Addition to the Curriculum
 Special Needs (Workshop, seminar, special topic, ...94 series, etc.)
4. Level of Instruction: Undergraduate Graduate (/G) Both
5. Credit Hours: 3.00
6. Is this course cross-listed with another department? NO
 If so, list the cross-listed catalog number (s)? _____
7. What session(s) will the course be offered? Fall Spring Summer All
8. What will be the yearly cycle for this course?
 All Years Even Years Odd Years One (1) Term Only
9. First term and year for this course: Fall 2020-2021 Length of Instruction (Weeks): 16 Weeks
10. Prerequisites:
 - A. Instructor / Advisor consent required? Yes No
 - B. Prerequisites Catalog # Prerequisite Course Title

| | |
|-------------|-------------|
| <u>NONE</u> | <u>NONE</u> |
| _____ | _____ |
| _____ | _____ |
 - C. Additional Prerequisites: NONE



11. **CATALOG DESCRIPTION:** Cybersecurity has become a topic of critical importance in today's networked and interconnected environment. The study of Cybersecurity Management describes the tools, techniques, methods, and strategies used by information security professionals and managers to combat security breaches and threats. This course provides an overview of the field of information security and in-depth knowledge of the complex nature of cyber threats and countermeasures. In this course students will examine key strategies and methodologies used to increase information continuity in business and government organizations and information security disaster preparedness. Also presented are methods of securing information systems using organizational security controls, policies, and best practices with coverage extended to additional topics including information privacy and regulations.
12. **DESCRIBE LIBRARY AND INFORMATION TECHNOLOGY RESOURCES AVAILABLE TO SUPPORT COURSE:** If insufficient library sources are available, describe alternatives that will be used. **Current learning resource holdings at the UOG-RFK Library and access to relevant periodicals are satisfactory to start up this course. Additional course-related material is available on-line. A course website will be designed by the instructor for this course that will be available to students upon enrollment. Additional resources will be available on the course Website, as well as, links to course-related material.**
13. **SUBSTANTIATE THE COMPELLING NEED FOR THE NEW COURSE:** **Organization leaders in business and government are becoming more aware of the risks and costs associated with managing, securing and protecting data and information in the workplace. In modern organizations - dependent on information technology, managers need to be aware of cyber threats and be able to develop plans and solutions to deal with these threats. With the growing dependence on data stored and shared by organizations, managers need to be knowledgeable about cybersecurity tools and techniques to address these issues. The knowledge learned in this class will help enhance the job opportunities and career advancement of students.**
14. **WHAT IS THE ANTICIPATED CLASS SIZE AND DOCUMENT INDICATIONS ON HOW THE NEW COURSE WILL MEET ITS PROJECTED SIZE.** **It is estimated that between 20-30 students and Cybersecurity Certificate participants will initially enroll in this course based on discussions and a survey with students, alumni and potential participants from government and business organizations on Guam and in the region. A public information initiative directed at UOG students and business and government organizations will precede the offering of this course and other new cybersecurity management courses prior to the start of the Fall Semester 2020-2021.**
15. **STATE HOW THE NEW COURSE WILL BE COVERED BY EXISTING PROGRAM FACULTY.** **The School of Business and Public Administration has excellent faculty resources to support this new course and other courses in the CJ-CSM Minor and Certificate program. Existing and new Full-Time SBPA faculty in the PALS and Business programs will teach this course and other courses in the CJ-CSM Minor and Certificate program. Qualified Adjuncts from professional business and government organizations on Guam, as well as, visiting Professors and faculty colleagues from sister colleges and schools at UOG may be invited to participate on an as-needed basis. SBPA has Full-Time and Adjunct faculty resources adept in information technology, forensics, law enforcement, policy-making and the law who desire to participate in course delivery.**









UNIVERSITY OF GUAM
Unibetsedåt Guåhan

Office of Academic and Student Affairs

- 16. **ADDITIONAL INFORMATION:** Please refer to the “Cybersecurity Management and Professional Certificate Program in Cybersecurity Management Proposal” document and Course Syllabi.
- 17. **ATTACH COURSE OUTLINE:** Please see attached Course Outline. Also refer to the CJ-CSM 300 Syllabus submitted with the proposal packet.

APPROVAL RECOMMENDED BY:

| UNIT | SIGNATURE (use BLUE pen please) | DATE |
|---|---|------------|
| For Program |  | 12/10/19 |
| Administrative Chair |  | 12/10/19 |
| Chair, College AAC/CC |  | 2/4/2020 |
| Dean, of College |  Dr. Annette T. Santos, Dean, SBPA | 2/4/2020 |
| UCRC/GCRC | Dr. Michael Hemmingsen  | 5/14/2020 |
| President, Faculty Senate (if substantive) |  (Endorsement of UCRC/GCRC Recommendation) | 05/14/2020 |

APPROVED:


 SENIOR VICE PRESIDENT
 ACADEMIC & STUDENT AFFAIRS

Jun 1, 2020
 DATE



REQUEST FOR NEW COURSE

1. Title: CYBERCRIME AND DIGITAL FORENSICS
2. Catalog Number: ^{FE} CJ-CSM 301 (New course may not duplicate active or inactive course number.)
3. Course Type:
 - Addition to the Curriculum
 - Special Needs (Workshop, seminar, special topic,...94 series, etc.)
4. Level of Instruction:
 - Undergraduate
 - Graduate (/G)
 - Both
5. Credit Hours: 3.00
6. Is this course cross-listed with another department? NO
 If so, list the cross-listed catalog number (s)? _____
7. What session(s) will the course be offered?
 - Fall
 - Spring
 - Summer
 - All
8. What will be the yearly cycle for this course?
 - All Years
 - Even Years
 - Odd Years
 - One (1) Term Only
9. First term and year for this course: Fall 2020-2021 Length of Instruction (Weeks): 16 Weeks
10. Prerequisites:
 - A. Instructor / Advisor consent required?
 - Yes
 - No
 - B. Prerequisites Catalog # Prerequisite Course Title

| | |
|-------------|-------------|
| <u>NONE</u> | <u>NONE</u> |
| _____ | _____ |
| _____ | _____ |
 - C. Additional Prerequisites: NONE



11. **CATALOG DESCRIPTION:** The global reach of the Internet, the low marginal cost of On-line activity, and the relative anonymity of information technology users have contributed to a wide escalation in cybercrimes. Consequently, information and communication technologies (ICT) are being increasingly employed to instigate threats to government, business and global economies. This course provides an overview of cybercrime and the forensic and digital law enforcement practices put in place to respond to them. The course will focus on the types and extent of current cybercrimes, how organizations respond to these crimes, including protections afforded to computer users, the policies that govern cybercrime detection and prosecution, and related law enforcement technologies.
12. **DESCRIBE LIBRARY AND INFORMATION TECHNOLOGY RESOURCES AVAILABLE TO SUPPORT COURSE:** If insufficient library sources are available, describe alternatives that will be used.
Current learning resource holdings at the UOG-RFK Library and access to relevant periodicals are satisfactory to start up this course. Additional course-related material is available on-line. A course website will be designed by the instructor for this course that will be available to students upon enrollment. Additional resources will be available on the course Website, as well as, links to course-related material.
13. **SUBSTANTIATE THE COMPELLING NEED FOR THE NEW COURSE:** Organization leaders in business and government are becoming more aware of the risks and costs associated with managing, securing and protecting data and information in the workplace. In modern organizations - dependent on information technology, managers need to be aware of cyber threats and be able to develop plans and solutions to deal with these threats. With the growing dependence on data stored and shared by organizations, managers need to be knowledgeable about cybersecurity tools and techniques to address these issues. The knowledge learned in this class will help enhance the job opportunities and career advancement of students.
14. **WHAT IS THE ANTICIPATED CLASS SIZE AND DOCUMENT INDICATIONS ON HOW THE NEW COURSE WILL MEET ITS PROJECTED SIZE.** It is estimated that between 20-30 students and Cybersecurity Certificate participants will initially enroll in this course based on discussions and a survey with students, alumni and potential participants from government and business organizations on Guam and in the region. A public information initiative directed at UOG students and business and government organizations will precede the offering of this course and other new cybersecurity management courses prior to the start of the Fall Semester 2020-2021.
15. **STATE HOW THE NEW COURSE WILL BE COVERED BY EXISTING PROGRAM FACULTY.** The School of Business and Public Administration has excellent faculty resources to support this new course and other courses in the CJ-CSM Minor and Certificate program. Existing and new Full-Time SBPA faculty in the PALS and Business programs will teach this course and other courses in the CJ-CSM Minor and Certificate program. Qualified Adjuncts from professional business and government organizations on Guam, as well as, visiting Professors and faculty colleagues from sister colleges and schools at UOG may be invited to participate on an as-needed basis. SBPA has Full-Time and Adjunct faculty resources adept in information technology, forensics, law enforcement, policy-making and the law who desire to participate in course delivery.






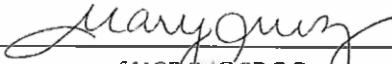


UNIVERSITY OF GUAM
Unibetsedät Guåhan

Office of Academic and Student Affairs

- 16. **ADDITIONAL INFORMATION:** Please refer to the “Cybersecurity Management and Professional Certificate Program in Cybersecurity Management Proposal” document and Course Syllabi.
- 17. **ATTACH COURSE OUTLINE:** Please see attached Course Outline. Also refer to the CJ-CSM 300 Syllabus submitted with the proposal packet.

APPROVAL RECOMMENDED BY:

| UNIT | SIGNATURE (use BLUE pen please) | DATE |
|---|---|------------|
| For Program |  | 12/10/19 |
| Administrative Chair |  | 12/10/19 |
| Chair, College AAC/CC |  | 2/4/2020 |
| Dean, of College |  Dr. Annette T. Santos, Dean, SBPA | 2/4/2020 |
| UCRC/GCRC | Dr. Michael Hemmingsen  | 5/14/2020 |
| President, Faculty Senate (if substantive) |  (Endorsement of UCRC/GCRC Recommendation) | 05/14/2020 |

APPROVED:

Anita Gorra Enriquez (Jun 1, 2020 20:49 GMT+10)
 SENIOR VICE PRESIDENT
 ACADEMIC & STUDENT AFFAIRS

Jun 1, 2020
 DATE



REQUEST FOR NEW COURSE

1. Title: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives
2. Catalog Number: CJ-CSM 302 (New course may not duplicate active or inactive course number.)
3. Course Type:
 - Addition to the Curriculum
 - Special Needs (Workshop, seminar, special topic, ...94 series, etc.)
4. Level of Instruction:
 - Undergraduate
 - Graduate (/G)
 - Both
5. Credit Hours: 3.00
6. Is this course cross-listed with another department? NO
 If so, list the cross-listed catalog number (s)? _____
7. What session(s) will the course be offered?
 - Fall
 - Spring
 - Summer
 - All
8. What will be the yearly cycle for this course?
 - All Years
 - Even Years
 - Odd Years
 - One (1) Term Only
9. First term and year for this course: Fall 2020-2021 Length of Instruction (Weeks): 16 Weeks
10. Prerequisites:
 - A. Instructor / Advisor consent required?
 - Yes
 - No
 - B. Prerequisites Catalog # Prerequisite Course Title

| | |
|-------------|-------------|
| <u>NONE</u> | <u>NONE</u> |
| _____ | _____ |
| _____ | _____ |
 - C. Additional Prerequisites: NONE



11. **CATALOG DESCRIPTION:** This course will introduce students to the key issues in cybersecurity management and the Law and help them develop a basic understanding of the technical, legal and ethical issues related to cybersecurity. Case studies in cybersecurity breaches and their legal consequences shall be presented, discussed and analyzed in this course. At the end of the course, students will understand today's cybersecurity legal and privacy-related challenges faced by leaders and managers of public and business organizations (Local, National and International).
12. **DESCRIBE LIBRARY AND INFORMATION TECHNOLOGY RESOURCES AVAILABLE TO SUPPORT COURSE:** If insufficient library sources are available, describe alternatives that will be used.
Current learning resource holdings at the UOG-RFK Library and access to relevant periodicals are satisfactory to start up this course. Additional course-related material is available on-line. A course website will be designed by the instructor for this course that will be available to students upon enrollment. Additional resources will be available on the course Website, as well as, links to course-related material.
13. **SUBSTANTIATE THE COMPELLING NEED FOR THE NEW COURSE:** **Organization leaders in business and government are becoming more aware of the risks and costs associated with managing, securing and protecting data and information in the workplace. In modern organizations - dependent on information technology, managers need to be aware of cyber threats and be able to develop plans and solutions to deal with these threats. With the growing dependence on data stored and shared by organizations, managers need to be knowledgeable about cybersecurity tools, techniques and the law, to address these issues. The knowledge learned in this class will help enhance the job opportunities and career advancement of students.**
14. **WHAT IS THE ANTICIPATED CLASS SIZE AND DOCUMENT INDICATIONS ON HOW THE NEW COURSE WILL MEET ITS PROJECTED SIZE.** It is estimated that between 20-30 students and Cybersecurity Certificate participants will initially enroll in this course based on discussions and a survey with students, alumni and potential participants from government and business organizations on Guam and in the region. A public information initiative directed at UOG students and business and government organizations will precede the offering of this course and other new cybersecurity management courses prior to the start of the Fall Semester 2020-2021.
15. **STATE HOW THE NEW COURSE WILL BE COVERED BY EXISTING PROGRAM FACULTY.** The School of Business and Public Administration has excellent faculty resources to support this new course and other courses in the CJ-CSM Minor and Certificate program. Existing and new Full-Time SBPA faculty in the PALS and Business programs will teach this course and other courses in the CJ-CSM Minor and Certificate program. Qualified Adjuncts from professional business and government organizations on Guam, as well as, visiting Professors and faculty colleagues from sister colleges and schools at UOG may be invited to participate on an as-needed basis. SBPA has Full-Time and Adjunct faculty resources adept in information technology, forensics, law enforcement, policy-making and the law who desire to participate in course delivery.
16. **ADDITIONAL INFORMATION:** Please refer to the "Cybersecurity Management and Professional Certificate Program in Cybersecurity Management Proposal" document and Course Syllabi.






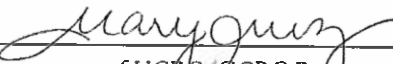


UNIVERSITY OF GUAM
Unibetsedät Guåhan

Office of Academic and Student Affairs

17. ATTACH COURSE OUTLINE: **Please see attached Course Outline. Also refer to the CJ-CSM 301 Syllabus submitted with the proposal packet.**

APPROVAL RECOMMENDED BY:

| UNIT | SIGNATURE (use BLUE pen please) | DATE |
|---|---|------------|
| For Program |  | 12/10/19 |
| Administrative Chair |  | 12/10/19 |
| Chair, College AAC/CC |  | 2/4/2020 |
| Dean, of College |  Dr. Annette T. Santos, Dean, SBPA | 2/4/2020 |
| UCRC/GCRC | Dr. Michael Hemmingsen  | 5/14/2020 |
| President, Faculty Senate (if substantive) |  (Endorsement of UCRC/GCRC Recommendation) | 05/14/2020 |

APPROVED:

Anita Gorja Enriquez (Jun 1, 2020 20:49 GMT+10)

**SENIOR VICE PRESIDENT
 ACADEMIC & STUDENT AFFAIRS**

Jun 1, 2020

DATE

REQUEST FOR NEW COURSE OUTLINE

(UOG Form)

- **CJ-CSM 100:** Introduction to Cybersecurity Management
- **CJ-CSM 200:** Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet
- **CJ-CSM 300:** Cybersecurity Management Tools and Techniques
- **CJ-CSM 301:** Cybercrime and Digital Forensics
- **CJ-CSM 302:** Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives



UNIVERSITY OF GUAM
Unibetsedät Guåhan

Office of Academic and Student Affairs

NEW COURSE OUTLINE FORM

College: School of Business and Public Administration Course Number: ~~CJ~~-CSM 100 *JE*

Course Title: Introduction to Cybersecurity Management Credit Hours: 3.00

Date of Final Approval: _____ Semester Offered: Fall/Spring/Summer

Course counts as:

| | | |
|---|--|---|
| | | general education requirement |
| √ | | part of <u>Criminal Justice</u> program |
| √ | | elective |

1. Catalog Description:

This course introduces students to the growing legal, technical, managerial, economic and social issues surrounding crimes committed in cyberspace. The course discusses the nature of cybercrime from a management and international perspective and focuses on how the borderless nature of cybercrime impacts law enforcement and cybersecurity in public and business organizations.

2. Course Content:

This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created. Students will examine the history and complex nature of computer-related cybercrime and how societies have attempted to respond. Students will discuss the different types of cybercriminals, including motives, rationale, and methods of attack. The course will also evaluate various legal and regulatory issues in cyberspace, including surveillance, sting operations, current and proposed legislation, user-reporting initiatives, identity filtering/blocking technologies, vigilante movements, individual rights and international law enforcement cooperation.

3. Rationale for the Course:

To provide students with a practical understanding and the opportunity to explore issues surrounding crimes committed in cyberspace that they need to prepare to manage in their careers and professions.

4. Skills and Background Required or Expected:

Students should have interest in cybersecurity management and basic computing, research and writing skills. Students should be committed to scholarly excellence and critical and creative engagement in all class activities.



5. Teaching Methodologies and Anticipated class size:

Lectures, class presentations, hands-on assisted information technology exercises and computer-simulations. Class size is anticipated to be 20-30 students.

6. Learning Objectives for Students:

(SLO 1) distinguish between the different types of cybercrimes, including who/what they target, how/where they are conducted, and why they persist.

(SLO 2) describe the impacts of the Internet on the opportunities created for committing traditional crimes (e.g., bullying) and new crimes (e.g., phishing).

(SLO 3) identify the challenges faced locally, nationally and internationally at combating cybercrime and the steps taken by managers in organizations to address these challenges.

(SLO 4) learn to take steps to increase individual security and privacy when online.

(SLO 5) take what has been learned in class and apply it to current organizational challenges and to their professional careers.

7. Methods of Evaluation

Tests, exercise simulations, writing and research assignments.

8. Methods for Student Learning Outcomes Assessment:

Pre and Post assessments will be used to measure student learning outcomes and to ensure students have achieved smart learning objectives.

9. Required and Recommended Texts or Study Guides:

Yar, M. (2013). *Cybercrime and Society (2nd Edition)*. Sage Publications. ISBN13: 978-1-4462-0194-7.
Clough, J. (2015). *Principles of Cybercrime (2nd Edition)*. Cambridge University Press. ISBN13: 978-1-107698161.

10. Subsequent Courses:


- **CJ-CSM 200: Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet**
- **CJ-CSM 300: Cybersecurity Management Tools and Techniques**
- **CJ-CSM 301: Cybercrime and Digital Forensics**
- **CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives**



11. Additional Course Descriptors, if any:

**See Course Syllabus*

The Calendar of Assignments, Assessment Project, a Statement Concerning the “Americans with Disabilities Act” (ADA) Accommodations for Students, Attendance and Grading Policies are to be included in the course syllabus.

| | | | |
|---|--------------------------------------|---|-------------|
| <input checked="" type="checkbox"/> Approved | <input type="checkbox"/> Disapproved |  <small>Anita Gorja Enriquez (Jun 1, 2020 20:49 GMT+10)</small> | Jun 1, 2020 |
| Senior Vice President, Academic & Student Affairs | | | Date |



UNIVERSITY OF GUAM
Unibetsedåt Guåhan

Office of Academic and Student Affairs

NEW COURSE OUTLINE FORM

College: School of Business and Public Administration

Course Number: CJ-CSM 200 *JK*

Course Title: **Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet**

Credit Hours: 3.00

Date of Final Approval: _____

Semester Offered: Fall/Spring/Summer

Course counts as:

general education requirement

part of Criminal Justice program

elective

1. Catalog Description:

This course describes how virtually every computer is connected, or has the potential to be connected, to other computers are how computer technology is subject to cyber threats. When connected locally, they provide vital services such as print servers, file servers, CPU servers, and when connected externally, offer access to the Internet, world-wide-web, electronic mail and the Cloud. Millions of people worldwide have been exposed to the World Wide Web of computers and the information they provide. In this course, students will learn how information technologies work and how the explosion in the use of information technologies is as important to organizational leaders and managers as the more traditional foundations of computer science such as computer architecture, operating systems and programming.

2. Course Content:

This course provides students with a comprehensive understanding of networking technologies, concepts, and terminology about information technology and the daily tasks involved in managing and troubleshooting a computer network for cybersecurity threats.

3. Rationale for the Course:

To provide students with an understanding of computer hardware, networking, and the Internet and to learn how these are used in public and business organizations and the need to secure these technologies from cybersecurity threats.

4. Skills and Background Required or Expected:

Students should have an interest in information technology and computer hardware. Student should have skills in basic computing, writing and research, and to be committed to engagement in all class

activities.

5. Teaching Methodologies and Anticipated class size:

Lectures, class presentations, hands-on assisted information technology exercises and computer-simulations. Class size is anticipated to be 20-30 students.

6. Learning Objectives for Students:

In this course, students will learn:

- **To develop an understanding of the modern network technologies in common use today;**
- **To appreciate how computer networks can format and transfer data at high speed and over both local and wide area networks.**

7. Methods of Evaluation

Tests, exercise simulations, writing and research assignments.

8. Methods for Student Learning Outcomes Assessment:

Pre- and Post assessments will be used to measure student learning outcomes and to ensure students have achieved smart learning objectives.

9. Required and Recommended Texts or Study Guides:

10. Subsequent Courses:

- **CJ-CSM 300: Cybersecurity Management Tools and Techniques**
- **CJ-CSM 301: Cybercrime and Digital Forensics**
- **CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives**

11. Additional Course Descriptors, if any: **See Course Syllabus*

The Calendar of Assignments, Assessment Project, a Statement Concerning the "Americans with Disabilities Act" (ADA) Accommodations for Students, Attendance and Grading Policies are to be included in the course syllabus.

Approved Disapproved


Anita Barja Enriquez (Jun 1, 2020 20:49 GMT+10)

Senior Vice President, Academic & Student Affairs

Jun 1, 2020

Date



UNIVERSITY OF GUAM
Unibetsedåt Guåhan

Office of Academic and Student Affairs

NEW COURSE OUTLINE FORM

College: School of Business and Public Administration Course Number: ~~CJ~~-CSM 300 *Sc*

Course Title: Cybersecurity Management Tools and Techniques Credit Hours: 3.00

Date of Final Approval: _____ Semester Offered: Fall/Spring/Summer

Course counts as:

| | | |
|--|---|---|
| | √ | general education requirement |
| | √ | part of <u>Criminal Justice</u> program |
| | | elective |

1. Catalog Description:

Cybersecurity has become a topic of critical importance in today's networked and interconnected environment. The study of Cybersecurity Management describes the tools, techniques, methods, and strategies used by information security professionals and managers to combat security breaches and threats. This course provides an overview of the field of information security and in-depth knowledge of the complex nature of cyber threats and countermeasures. In this course students will examine key strategies and methodologies used to increase information continuity in business and government organizations and information security disaster preparedness. Also presented are methods of securing information systems using organizational security controls, policies, and best practices with coverage extended to additional topics including information privacy and regulations.

2. Course Content:

Students will learn about cybersecurity concepts, issues, tools and techniques that are critical for managers in organizations to know how to plan for, respond to, and solve problems in the computing security domain.

3. Rationale for the Course:

This course will provide students with an in-depth understanding of core concepts and applications with a focus on cybersecurity functional management competencies related to real life cybersecurity threats in public and business organizations.

4. Skills and Background Required or Expected:

Students should have an interest in information technology and computer hardware. Student should have skills in basic computing, writing and research, and to be committed to engagement in all class activities.



5. Teaching Methodologies and Anticipated class size:

Lectures, class presentations, hands-on assisted information technology exercises and computer-simulations. Class size is anticipated to be 20-30 students.

6. Learning Objectives for Students:

The course is aimed at imparting knowledge and skill sets required to assume the overall responsibilities of administration and management of the security function of an enterprise information system. After completing the course, students will be able to:

- Carry out a detailed analysis of enterprise information security by performing various types of analysis such as vulnerability analysis, penetration testing, audit trail analysis, system and network monitoring,
- Carry out detailed risk analysis and assessment of enterprise information systems using various practical tools and techniques.
- Design detailed enterprise-wide security plans and policies and deploy appropriate safeguards at all the levels in the organization by providing due consideration to the life cycle of the enterprise information systems and networks, as well as its legal and social environment.
- Identify and prioritize information assets
- Identify and prioritize threats to information assets
- Define an information security strategy
- Plan for and respond to intruders in an information system
- Describe legal and public relations implications of security and privacy issues
- Present a disaster recovery plan for recovery of information assets after an incident

7. Methods of Evaluation

Tests, exercise simulations, writing and research assignments.

8. Methods for Student Learning Outcomes Assessment:

Pre- and Post assessments will be used to measure student learning outcomes and to ensure students have achieved smart learning objectives.

9. Required and Recommended Texts or Study Guides:

- Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*, 2016.
- Micki Krause, Harold F. Tipton, *Handbook of Information Security Management*, 2017.
- *Guide to Disaster Recovery*, M. Erbschilde, 2015.
- *Guide to Network Defense and Countermeasures*, G. Holden., 2017.
- *Computer Security: Art and Science*, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2013.




10. Subsequent Courses:

- **CJ-CSM 301: Cybercrime and Digital Forensics**
- **CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives**

11. Additional Course Descriptors, if any: **See Course Syllabus*

Accommodations for Students, Attendance and Grading Policies are to be included in the course syllabus.

The Calendar of Assignments, Assessment Project, a Statement Concerning the "Americans with Disabilities Act" (ADA)

| | | |
|---|--|---------------------|
| <input checked="" type="checkbox"/> Approved <input type="checkbox"/> Disapproved |  <small>Anita Borja Enriquez (Jun 1, 2020 20:49 GMT+10)</small> Senior Vice President, Academic & Student Affairs | Jun 1, 2020 Date |
|---|--|---------------------|



UNIVERSITY OF GUAM
Unibetsedåt Guåhan

Office of Academic and Student Affairs

NEW COURSE OUTLINE FORM

College: School of Business and Public Administration Course Number: CJ-CSM 301 *JE*

Course Title: Cybercrime and Digital Forensics Credit Hours: 3.00

Date of Final Approval: _____ Semester Offered: Fall/Spring/Summer

Course counts as:

| | |
|---|---|
| | general education requirement |
| √ | part of <u>Criminal Justice</u> program |
| √ | elective |

1. Catalog Description:

The global reach of the Internet, the low marginal cost of On-line activity, and the relative anonymity of information technology users have contributed to a wide escalation in cybercrimes. Consequently, information and communication technologies (ICT) are being increasingly employed to instigate threats to global civil society. This course provides an overview of cybercrime and the forensic and digital law enforcement practices put in place to respond to them. The course will focus on the types and extent of current cybercrimes, how organizations respond to these crimes, including protections afforded to computer users, the policies that govern cybercrime detection and prosecution, and related law enforcement technologies.

2. Course Content:

Technology, cybercrime, and police investigations, computer misuse crimes and investigations, hacking, malware and automated computer attacks, digital piracy and IP theft, economic and financial crimes, pornography, prostitution, and sex crimes, cyberbullying and on-line harassment and cyberstalking, voyeurism, revenge pornography, and vice crimes (on-line gambling), digital and computer forensics, on-line extremism, cyberattacks, mutual law enforcement assistance agreements (Local, National and International).

3. Rationale for the Course:

This course will provide students with an understanding of various types of cybercrimes experienced in public and business organizations. Forensic techniques used in law enforcement are identified. Students are taught how to manage cyber threats and intrusions in organizations.

4. Skills and Background Required or Expected:

Students should demonstrate an interest in cybersecurity management and in solving and managing cybercrime intrusions in public and business organizations. Students should have basic computing,



writing and research skills, and to be committed to engagement in all class activities.

5. Teaching Methodologies and Anticipated class size:

Lectures, class presentations, hands-on computer forensic exercises and computer-assisted forensic simulations. Class size is anticipated to be 20-30 students. Students are expected to enroll in this class.

6. Learning Objectives for Students:

- Define and describe the nature and scope of cybercrime;
- Develop knowledge of major types and incidents of cybercrime and their resulting impact;
- Analyze and discuss national and global digital law enforcement efforts;
- Critically consider procedures governing cybercrime forensics, detection and prosecution;
- Identify and evaluate the specific technology that facilitates cybercrime forensics and digital law enforcement;
- Critically evaluate the impact of cybercrime on public and business organizations

7. Methods of Evaluation

Tests, forensic exercise technology simulations, writing and research assignments.

8. Methods for Student Learning Outcomes Assessment:

Pre- and Post assessments will be used to measure student learning outcomes and to ensure students have achieved student learning objectives.

9. Required and Recommended Texts or Study Guides:

- Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellat. 2015. *Cybercrime and Digital Forensics: An Introduction*. New York: Routledge. ISBN: 978-1138021303.
- Nate Anderson. 2014 *The Internet Police: How Crime Went Online, and the Cops Followed*. New York: W.W. Norton & Company, Inc. ISBN: 978-0393349450.


10. Subsequent Courses:

- **CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives**

11. Additional Course Descriptors, if any: **See Course Syllabus*



The Calendar of Assignments, Assessment Project, a Statement Concerning the “Americans with Disabilities Act” (ADA) Accommodations for Students, Attendance and Grading Policies are to be included in the course syllabus.

| | | | |
|--|--------------------------------------|--|-------------|
| <input checked="" type="checkbox"/> Approved | <input type="checkbox"/> Disapproved |  <small>Anita B. Enriquez (Jun 1, 2020 20:49 GMT+10)</small> | Jun 1, 2020 |
| | | Senior Vice President, Academic & Student Affairs | Date |



UNIVERSITY OF GUAM
Unibetsedât Guåhan

Office of Academic and Student Affairs

NEW COURSE OUTLINE FORM

College: School of Business and Public Administration Course Number: ~~CJ~~-CSM 302 *JK*

Course Title: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives

Credit Hours: 3.00

Date of Final Approval: _____ Semester Offered: Fall/Spring/Summer

Course counts as:

| | |
|---|---|
| | general education requirement |
| √ | part of <u>Criminal Justice</u> program |
| | elective |
| √ | |

1. Catalog Description:

This course will introduce students to the key issues in cybersecurity management and the law, and help them develop a basic understanding of the technical, legal and ethical issues related to cybersecurity. Case studies in security breaches and their legal consequences shall be presented, discussed and analyzed in this course. At the end of the course, students will understand today's cybersecurity legal and privacy-related challenges faced by leaders and managers of public and business organizations.

2. Course Content:

Need for Cybersecurity Law, Cyber Law from the Local, National and International Perspective and legal case reviews. Constitutional and Human Rights issues in Cyberspace, Cybercrimes and the legal framework; Cyber Torts (Defamation and Civil wrongs); Intellectual Property issues in cyberspace; E-Commerce and the Law; Digital Resolution in Cyberspace; Public policy and legal responses to cybercrime.

3. Rationale for the Course:

This course will provide students with an understanding of the law and legal framework that guides attorneys and managers in investigating, managing and prosecuting cybercrimes at the local, national and international level.

4. Skills and Background Required or Expected:

Students should demonstrate an interest in law as it applies to cybersecurity, cybercrime, cyberthreats and cyberintrusions as it impacts public and business organizations. Students should be able to



research and analyze legal cases in cybersecurity and have good writing skills.

5. Teaching Methodologies and Anticipated class size:

Lectures, class presentations, and legal case reviews. Class size is anticipated to be 20-30 students.

6. Learning Objectives for Students:

- Learn the key applications and issues in cybersecurity and the law
- Develop an understanding of the legal and ethical issues related to cybersecurity management and cybercrime
- Learn to research and analyze legal cases in cybersecurity, cybercrime and cyberresponses
- Understand the legal consequences of organization management of private information
- Understand today's cybersecurity challenges at the local, national and international level.

7. Methods of Evaluation

Tests; Case study research and reviews; research papers.

8. Methods for Student Learning Outcomes Assessment:

Pre- and Post assessments will be used to measure student learning outcomes and to ensure students have achieved student learning objectives.

9. Required and Recommended Texts or Study Guides:

- Chris Reed & John Angel, *Computer Law*, OUP, New York, (2007).
- Jonathan Rosenoer, *Cyber Law*, Springer, New York, (1997).

References:

- *Cybersecurity for Executives: A Practical Guide*, Gregory J. Touhill; Wiley, 2014
- *Privacy Program Management: Tools for Managing Privacy within*.
- Singer, P.W. and Allan Friedman, 2014. *Cybersecurity and Cyberwar* (Oxford University Press).
- Clarke, Richard and Robert K. Knake, 2010. *Cyber War* (New York: Harper Collins).


Supplied On-line by Instructor: Handouts, including legal cases, exercises and articles.

10. Subsequent Courses: None.

11. Additional Course Descriptors, if any: *See Course Syllabus



The Calendar of Assignments, Assessment Project, a Statement Concerning the “Americans with Disabilities Act” (ADA) Accommodations for Students, Attendance and Grading Policies are to be included in the course syllabus.

| | | | |
|---|--------------------------------------|---|-------------|
| <input checked="" type="checkbox"/> Approved | <input type="checkbox"/> Disapproved |  <small>Anita R. de la Encarnación (Jun 1, 2020 20:49 GMT+10)</small> | Jun 1, 2020 |
| Senior Vice President, Academic & Student Affairs | | | Date |

Course Syllabus for Cybersecurity Management Minor and Professional Certificate Program

- CJ-CSM 100: Introduction to Cybersecurity Management
- CJ-CSM 200: Fundamentals of Computers and Networking Technologies for Cybersecurity Managers in Organizations: Understanding Computer Hardware, Networks and the Internet
- CJ-CSM 300: Cybersecurity Management Tools and Techniques
- CJ-CSM 301: Cybercrime and Digital Forensics
- CJ-CSM 302: Legal Issues and Cases in Cybersecurity and the Law: Local, National and International Perspectives



Introduction to Cybersecurity Management Course Syllabus

UNIVERSITY OF GUAM
Unibetsedåt Guahan

School of Business and Public Administration

Course and Contact information

Instructor: _____
Location: _____
Office: _____
Office hours: _____
Office Telephone: _____
Email: _____

1. PREREQUISITES:

This course is open to all UOG students and Cybersecurity Management Certificate Program participants.

2. CATALOG DESCRIPTION:

This course introduces students to the growing legal, technical and security management issues surrounding crimes committed in cyberspace or assisted by computers. The course discusses the nature of cybercrime from a management and international perspective and how the borderless nature of cybercrime impacts regulation and enforcement.

3. COURSE DESCRIPTION:

This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created. Students will examine the history and complex nature of computer-related cybercrime and how societies have attempted to respond. Students will discuss the different types of cybercriminals, including motives, rationale and methods of attack. The course will also evaluate various legal and regulatory issues in cyberspace, including surveillance, sting operations, current and proposed legislation, user-reporting initiatives, identify filtering/blocking technologies, vigilante movements, individual rights and international law enforcement cooperation.

4. COURSE GOALS:

The UOG Public Administration and Legal Studies Program is committed to scholarly excellence. Therefore, the PALS program promotes academic, critical and creative engagement with language (i.e., reading and writing) throughout its curriculum. A sustained and intensive exploration of language prepares students to think critically and to act meaningfully in interrelated areas of their lives – personal, professional, economic, social, political, ethical and cultural. It is intended that graduates of PALS programs leave the University prepared to enter a range of careers and for advanced study in a variety of fields; they are prepared to more effectively identify and ameliorate critical issues in their personal, professional and civic lives. Indeed, the impact of literacy is evident not only within the span of a specific, or academic degree or program, but also over the span of a lifetime.

5. STUDENT LEARNING OUTCOMES (SLOs)

Upon successful completion of this course, students will be able to:

- SLO 1: distinguish between the different types of cybercrimes, including who/what they target, how/where they are conducted and why they persist.
- SLO2: describe the impacts of the Internet on the opportunities created for committing traditional crimes (e.g., bullying) and new crimes (e.g., phishing).
- SLO3: identify the challenges faced locally, nationally and internationally at combating cybercrime and the steps taken by managers in organizations to address these challenges.
- SLO4: takes steps to increase their own security and privacy when online.
- SLO5: take what they have learned in class and apply it to current events and to their professional careers.

6. REQUIRED TEXTS/READINGS

Textbooks:

Yar, M. (2013). *Cybercrime and Society* (2nd Edition). Sage Publications. ISBN13: 978-1-4462-0194-7.

Clough, J. (2015). *Principles of Cybercrime* (2nd Edition). Cambridge University Press. ISBN13: 978-1-107698161.

Other Readings:

May be supplied electronically or in hardcopy format.

7. COURSE REQUIREMENTS AND ASSIGNMENTS

Discussion (30%): Each week there will be class discussion on specific readings and key issues or current events related to that week's overall topic. Students will be expected to provide their viewpoint and critically discuss the implications of the issue or event to their understanding of cybercrime and how it is addressed by organization managers and societies. This assignment will specifically address SLO's 3, 4 and 5.

Paper #1 – Online Privacy (20%): The purpose of this assignment is to provide students with practical experience to explore the concept of personal privacy, or lack thereof, on the Internet. Students will write a short six to eight-page paper (excluding title page and references) on their investigation of two topics. First, students will input their name into a search engine, with minimal other identifying information, and describe whether the data returned was about them, and how they felt about that information being readily accessible. They will describe the age (i.e., how old), personal nature (e.g., address, phone number, banking information), and online profile (e.g., your likes/dislikes, purchases, hobbies) it presented about them. Second, students will be required to use any cyber methods they can devise to find information on the course instructor. Students will be required to record the steps they took (e.g., search terms) to acquire the information and what information they obtained, including where it was found. Students will then describe this process and reflect on the steps others may take to find out personal information about them. This assignment will specifically address SLO 4.

Paper #2 – Combatting Cybercrime Locally, Nationally and Internationally: The purpose of this assignment is for students to explore the legal issues regarding how governments and social control

agencies can police a virtual environment without physical boundaries and borders. Select a type of cybercrime discussed in the course and determine how partnerships/cooperation/resource-sharing could, realistically, be improved between them and others. Students will write a short six to eight-page paper (excluding title page and references) on the laws, if any, that exist in each country and what each could learn from the other. Discussion should include how privacy and rights can be balanced with security. This assignment will specifically address SLO's 3 and 4.

Final Examination (30%): Students will be administered a final examination worth 30% of their final grade. Exam is closed book and will cover material from lectures and student presentations. The final exam may be comprised of multiple choice and short essay answer questions. The examinations will specifically address SLO's 1, 2 and 3.

Grading Information

- In order to receive a grade for this course, all course requirements must be met, and every assignment must be completed. Failure to complete any one assignment may result in a failing grade for this course.
- Individual assignment rubrics will be provided.
- Late assignments/papers will lose 10% for every calendar day that they are late, including weekend days.

Determination of Grades

| | | | | | |
|----------|-------------|---|-------------|-----------|-------------|
| A (plus) | 97% - 100% | A | 93% - < 97% | A (minus) | 90% - < 93% |
| B (plus) | 85% - < 90% | B | 80% - < 85% | B (minus) | 75% - < 80% |
| C (plus) | 71% - < 75% | C | 67% - < 71% | C (minus) | 63% - < 67% |
| D (plus) | 59% - < 63% | D | 54% - < 59% | D (minus) | 50% - < 54% |
| F | Below 50% | | | | |

University Policies

University-wide policy information relevant to all courses will apply in this class such as academic integrity, accommodations, etc. (See UOG Student Handbook and UOG Catalog for guidance).

**CJ-CSM 100: Introduction to Cybersecurity Management
Course Schedule and Topics**

This course schedule is subject to change with fair notice, at the instructor's discretion. All reading assignments listed should be completed prior to class on that date. Additional readings may be assigned.

| Week | Date | Topics | Readings |
|-------------|-------------|---|---|
| 1 | | Introduction -Course Overview -Assignments | <i>Principles of Cybercrime (Clough)</i> Chapter 1 (Cybercrime) <i>Articles</i> The Current State of Cybercrime Scholarship (Holt & Bossler) The Internet as a Conduit for Criminal Activity (Wall) |
| 2 | | What is Cybercrime -Computer and Internet basics -Cybercrime in research -Routine activity Theory | <i>Cybercrime and Society (Yar)</i> Chapter 1 (Cybercrime and the Internet) <i>Principles of Cybercrime (Clough)</i> Chapter 2 (Computer as Target) <i>Articles</i> How does the Internet work (Strickland) How Firewalls Work (Tyson) What is an 'IP Address' (Gil) |
| 3 | | Malware -Viruses, worms, trojan horses, rootkits, keyloggers & ransomware | <i>Principles of Cybercrime (Clough)</i> Chapter 4 (Modification or Impairment of Data) <i>Articles</i> Mobile Malware Evolution 2016 (Kaspersky Lab) Internet Security Report 2017 (ISTR) |
| 4 | | Hacking -Hacker culture -Legal issues -Hacking as a service | <i>Cybercrime and Society (Yar)</i> Chapter 2 (Hackers, Crackers, and Viral Coders) <i>Articles</i> Hackers Manifesto (The Mentor) How Big and Powerful is Anonymous (Vandita) |
| 5 | | Copyright Infringement -What is copyright infringement? -Who owns the data on the Internet? -Piracy (peer-2-peer) | <i>Cybercrime and Society (Yar)</i> Chapter 4 (Virtual Pirates) <i>Principles of Cybercrime (Clough)</i> Chapter 8 (Criminal Copyright Infringement) <i>Articles</i> An Oral History of Napster (Fortune) |
| 6 | | Personal Security -Privacy -Surveillance -Personal safety -The Secret War | <i>Cybercrime and Society (Yar)</i> Chapter 10 (Cyberscrimes and Cyberliberties) <i>Articles</i> The Secret War (Popular Mechanics) The Online Threat (Hersh) |

| Week | Date | Topics | Readings |
|------|------|---|---|
| 7 | | Your Online ID -Social networks & search engines -Identity theft & fraud | <i>Cybercrime and Society (Yar)</i> Chapter 5 (Cyber-Frauds, Scams, and Cons) <i>Principles of Cybercrime (Clough)</i> Chapter 7 (Fraud) <i>Articles</i> What is Social Engineering (Webroot) |
| 8 | | Email Spam -Phishing & Pharming OLegal issues -Legislation efforts | <i>Principles of Cybercrime (Clough)</i> Chapter 9 ('Spam') Paper #1 (Tell Me a Story) Due |
| 9 | | Deep Web -TOR -Digital currency (Bitcoin) -The Dark Web | <i>Articles</i> Exploring the Deep Web (Trend Micro) TOR Project: Overview (TOR) What are BitCoins (Lifewire) How BitCoin Works (Forbes) |
| 10 | | Organized Crime -Carding -Money Laundering -Drugs & weapons | <i>Articles</i> Koobface: Inside a Crimeware Network (Villeneuve) The Great Cyberheist (Verini) A Hacker's Race to Build the Amazon.com of Stolen Credit Cards (WeiderWeb) Carders.cc Hacked (Reusablesec) |
| 11 | | Personal Cyber-Crimes -Stalking -Bullying | <i>Cybercrime and Society (Yar)</i> Chapter 8 (The Victimization of Individuals Online) <i>Principles of Cybercrime (Clough)</i> Chapter 12 (Harassment) & Chapter 13 (Voyeurism) |
| 12 | | Terrorism & Extremism -Terrorism in the digital age -Methods of distribution -Researching online terrorism (White Supremacists) | <i>Cybercrime and Society (Yar)</i> Chapter 3 (Political Hacking) <i>Articles</i> How Modern Terrorism Uses the Internet (Weimann) Terrorism and the Internet (Conway) Terror on the Internet (Tsfati & Weimann) Exploring Stormfront (Bowman-Grieve) |
| 13 | | Sex Crimes -Trafficking -child sexual exploitation -Sexting -Revenge pornography | <i>Cybercrime and Society (Yar)</i> Chapter 7 (Child Pornography and Child Sex Abuse Imagery) <i>Principles of Cybercrime (Clough)</i> Chapter 10 (Child Pornography) Chapter 11 (Grooming) <i>Articles</i> Fighting Human Trafficking (European Commission) Paper #2 (Combatting Cybercrime Internationally) Due |

| | | | |
|-----------|--|--|---|
| 14 | | Cybercrime and the Law -Patriot Act -International challenges -Jurisdiction -Joint operations | <i>Cybercrime and Society (Yar)</i> Chapter 9 (Policing the Internet) <i>Principles of Cybercrime (Clough)</i> Chapter 14 (Jurisdiction) Chapter 6 (Interception of Data) |
| 15 | | REVIEW | NO READINGS |
| 16 | | FINAL EXAMINATION | NO READINGS |



Fundamentals of Computers and Networking Technologies
Cybersecurity Managers: Computer Hardware, Networks,
and the Internet

COURSE SYLLABUS

UNIVERSITY OF GUAM

Unibetsedåt Guåhan

School of Business and Public Administration

Course and Contact information

Instructor: _____
Location: _____
Office: _____
Office hours: _____
Office Telephone: _____
Email: _____

1. CATALOG DESCRIPTION:

This course describes how virtually every computer is connected, or has the potential to be connected, to other computers. When connected locally, they provide vital services such as print servers, file servers, CPU servers and when connected externally, offer access to the Internet, world-wide-web, electronic mail and The Cloud. Millions of people worldwide have been exposed to the World Wide Web of computers and the information they provide.

Students will learn how the explosion in the use of technologies and local area networks has made the study of computer networks and the underlying communication technology by managers responsible for cybersecurity as important as the more traditional foundations of computer science such as computer architecture, operating systems and programming.

2. COURSE DESCRIPTION:

This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created. Students will examine the history and complex nature of computer-related cybercrime and how societies have attempted to respond. Students will discuss the different types of cybercriminals, including motives, rationale and methods of attack. The course will also evaluate various legal and regulatory issues in cyberspace, including surveillance, sting operations, current and proposed legislation, user-reporting initiatives, identify filtering/blocking technologies, vigilante movements, individual rights and international law enforcement cooperation.

3. COURSE OBJECTIVES:

The main goal of this course is to provide non-technical managers with a comprehensive understanding of networking technologies, concepts and terminology. Students will learn about the equipment and technologies used in LANs and WANs. They will learn about the network topologies used today and learn how to design a network using these topologies. A variety of network equipment will be discussed, including hubs, routers, switches, and NICs. LAN architectures are covered including Ethernet, Token

ring, and FDDI. Also, students will learn about wide area networking technologies and remote access technologies such as X.25, ISDN, frame relay, ATM, DSL, SMDS, and SONET networks. Wireless networking and handheld computer are also discussed. All major LAN and WAN protocols will be discussed including TCP/IP and the newer IPv6. In addition, students will learn about the OSI layered communications model. Aside from learning the technologies involved in networking. Students will get to understand the daily tasks involved with managing and troubleshooting a network.

4. COURSE GOALS:

In this course students will learn:

- To develop an understanding of the modern network technologies in common use today
- To appreciate how computer networks can format and transfer data at high speed and over both the local and wide are
- To identify potential and actual limitations with existing networks and identify advances in technology that may solve them

5. STUDENT LEARNING OUTCOMES (SLOs)

Upon successful completion of this course, students will be able to:

- demonstrate an understanding of the physical properties and performance characteristics of communication media; specifically, copper cable, fiber optics and wireless networks;
- demonstrate an understanding of the importance of communication standards, including an appreciation of protocol layer models and enhancements to those standards;
- demonstrate an appreciation of the theory and practice of common local area networks including virtual and wireless LANs;
- demonstrate an appreciation of the theory and practice of wide area networks and their interconnection;
- demonstrate an appreciation of the significance of network and inter-network protocols; specifically, IPv4, IPv6, TCP and UDP;
- describe the importance of reliability and quality of service in organizations including examples of information security, error recovery strategies, traffic differentiation and prioritization.

6. TEXTBOOKS

| Book Title | Author | ISBN | Publisher |
|--|------------|---------------|-------------------|
| Data Communications & Computer Networks: A Business User's Approach, 4 th Edition | Curt White | 0-619-16035-7 | Course Technology |

Recommended Reading List:

| Primary Texts | ISBN 10 | ISBN 13 |
|--|------------|----------------|
| Stallings, W. Data and Computer Communications. 10 th Edition. Pearson Education. 2013. | 1292014385 | 978-1292014388 |
| Tanenbaum, A. Computer Networks. 5 th Edition. Pearson Education. | 1292024224 | 978-1292024226 |

Other Texts:

| | | |
|---|------------|-----------------|
| Stallings, W. Wireless Communication and Networks. 2 nd Edition Pearson Education. 2013. | 129202738X | 978-129-2027388 |
|---|------------|-----------------|

Other Required Materials: The course will be enriched by demonstrations of various concepts covered and the media mix will include power points, video clips, audio clips, narrated demonstrations.

7. PRIOR KNOWLEDGE EXPECTED

Students are expected to be familiar with computer architectures, particularly regarding the representation of information within a computer system. Some practical exposure to local and wide area networks would be useful for context.

Detailed Course Evaluations:

| Percent | Item |
|-------------|----------------------|
| 30% | Lab/Homework/Quizzes |
| 30% | Midterm Exam |
| 40% | Final Exam |
| Total: 100% | |

The standard grading scale of 90-100% equals a B, 70-79% equals a C, 60-69% equals a D, and 0-59% equals an F.

Late Assignments Policy: Late assignments may be turned in within one week of due date with a 20% penalty. No assignments will be accepted after the final exam date!!!

Make-Up Exam Policy: Students are expected to take all exams on the scheduled days and submit all assignments by the deadline. Make-up exams are NOT guaranteed, but are granted at the discretion of the instructor. If make-up exams are necessary, it is necessary for students to make arrangements with the instructor *PRIOR* to exam date. **NOTE: There is NO make-up exam for the final.**

Format and Duration of the Final Examination

The examination is a one hour closed door examination (no materials can be taken into the examination room) based on the syllabus in this document.

8. BROAD COURSE OUTLINE: *Introduction to Hardware, Network, the Internet*

- I. Definition of computer system, Block Diagram, Components of a computer system, generations of computer, storage devices, Memory Hierarchy, Software, Classification of software, Operating System and its functionalities.
- II. Introduction to networking; Data communications: components, data representation (ASCII, ISO, etc.), direction of data flow (simplex, half duplex, full duplex); network criteria, physical structure (type of connection, topology), categories of network (LAN, MAN, WAN);

Internet: brief history, Protocols and standards; Reference models: OSI reference model, TCP/IP

reference model, their comparative study. Overview of data (analog & digital), signal (analog & digital), transmission (analog & digital) & transmission media (guided & unguided);

- III. Local Area Networks and data link protocols, point-to-point links and sliding window flow control, CSMA/CD, Ethernet, wireless LAN, cellular networks, and advanced multi-user communication (CDMA, SDMA/MIMO), mobility

Internetworking using TCP/IP: network programming using socket API, network client/server design;

Packet/circuit switching and wide-area networks: store-and-forward networks, source routing, virtual/permanent, circuits and call set-up, LAN/WAN addressing, hop-by-hop vs end-to-end control.

- IV. Routing techniques – intra-domain routing (OSPF, RIP), inter-domain policy routing (BGP) and network connectivity.

Transport protocols – TCP and UDP, Congestion control, TCP window control, multimedia streaming.

High-level network services – DNS, HTTP, SMTP, network management (SNMP), network security.

- V. Introduction and history of Internet, WWW, Markup Language: HTML, XML and tags, Scripting Languages, Client-Server Architecture, websites, Internet security and threats, Firewall, Introduction to e-commerce.

9. COURSE SCHEDULE AND TOPICS

| Week | Chapter Readings | Content |
|-------|---|---|
| 1 | Syllabus -Introduction to course Chapter 1 Introduction to Computer Networks and Data Communications. | Historical perspective, theoretical and practical models of network architecture particularly the ISO OSI seven-layer model and the TCP/IP protocol stack. Example networks and services including prototype new technologies. These would include Frame Relay, ISDN, ATM, Wi-Fi, xDSL, WiMAX, 2G and 3G. |
| 2 - 3 | Chapter 2 – Fundamentals of Data and Signals Chapter 3 – The Media: Conducted and Wireless | Physical properties of copper media, fiber optics, radio communication and data communication standards. Maximum data rates (theoretical and practical) for different media including some simple analysis of signals. Data encoding of digital signals. The distinction between and analysis of, physical media and wireless media properties. The difference between narrow band and broad band technologies with reference to ISDN and xDSL. |
| 4 – 5 | Chapter 4: Making Connections Chapter 5: Multiplexing: Sharing a Medium | |

| Week | Chapter Readings | Content |
|---------|---|---|
| 5 - 6 | Chapter 6: Errors, Error Detection, and Error Control | The main causes of errors and their effects on transmission. Single bit and burst errors. Various error detection and correction strategies including parity, block sum, Hamming Codes, Cyclic Redundancy Checks and Forward versus Backward error control. Statistical analysis of the effectiveness of error detection and correction code. |
| 7 - 8 | Chapter 7: Local Area Networks & The Basics Review for Midterm Exams MIDTERM EXAMS | Types of LAN covering standards, topology and performance. Example architectures such as Ethernet and fast Ethernet, ATM, and Wi-Fi. The operation of LAN switches and the configuration of virtual LANs. |
| 9 - 10 | Chapter 8: Local Area Networks – Internetworking Chapter 9: Local Area Networks – Software and Support Systems | |
| 11 - 12 | Chapter 10: Introduction to Wide Area Networks | Circuit versus packet switching and associated routing and flow control. Detailed examples of existing architectures such as Frame Relay, ISDN, ATM, Multi-protocol Label Switching (MPLS) and Virtual Private Networks (VPN). |
| 13 - 14 | Chapter 11: The Internet Chapter 12: Telecommunication Systems Chapter 13: Network Security | |
| 15 | Chapter 14: Network Design and Management/Quality of Service | A definition of quality of service and the main parameters that define network performance. Router functionality including frame prioritization, classification and queue management techniques. The provision of quality of service management in practical networks such as Frame Relay, ATM and the Internet. |
| 16 | Review for Final Exams | |
| 17 | FINAL EXAMS – PER UOG SCHEDULE | |

NOTICE: This schedule is subject to change based on class progress and the instructor's discretion.



CJ-CSM 300: CYBERSECURITY MANAGEMENT TOOLS AND TECHNIQUES

Log No. 6402

COURSE SYLLABUS

UNIVERSITY OF GUAM
Unibetseddåt Guåhan

School of Business and Public Administration

Course and Contact information

Instructor: _____
Location: _____
Office: _____
Office hours: _____
Office Telephone: _____
Email: _____

1. COURSE OVERVIEW:

Cybersecurity has become a topic of critical importance in today's networked and interconnected environment. The study of cybersecurity management describes the tools, techniques, methods, and strategies used by information security professionals to combat security breaches and threats. This course provides an overview of the field of information security and in-depth knowledge of the complex nature of related threats and countermeasures. Students examine key strategies and methodologies used to increase business and government continuity and disaster security preparedness. Also presented are methods of securing information systems using security controls, policies, and best practices with coverage extended to additional topics including information privacy and information security laws and regulations.

Computer security pervades every aspect of the modern online experience today, reaching into mobile phones and game consoles as well as conventional computer systems in organizations. This course covers some of the fundamental principles of cybersecurity management after identifying different aspects of cybersecurity information systems. A number of practical exercises and assignments will be given to students. For each assignment, the aim is to specify the requirements of a solution, explain an appropriate management tool to use, and then discuss pitfalls, cyberattacks and countermeasures. Students will learn how to detect threats, protect information systems and networks, and anticipate potential cyberattacks.

In this course students will be given an extensive overview of the various branches of computing security and will learn the concepts, issues and tools that are critical in solving problems in the computing security domain. Students will have the opportunity to learn essential techniques in protecting systems and network infrastructure, analyzing and monitoring potential cyberthreats and attacks, and devising and implementing security policies and solutions for public and private sector organizations. The duration of the course is one semester and its syllabus is divided into parts to provide students with an in-depth understanding of core concepts with a focus on functional management competencies related to real life cybersecurity threat situations.

2. COURSE/CATALOG DESCRIPTION:

This course covers issues related to the administration and management of information security systems in a public or private sector enterprise. The goal of the course is for managers who are not information technology professionals to learn and maintain an appropriate level of knowledge awareness and skill in cybersecurity tools and techniques to allow them to minimize the occurrence and severity of information security incidents in organizations. The students will learn the management needed techniques to plan for detect, respond to, and prevent computer network intrusions. Topics include how to lead and work with members of the I.T. Team in intrusion detection, vulnerability analysis, anomaly detection, computer forensics, auditing and data management, risk management contingency planning and incident handling and response. The course will also cover ethical and legal issues in information, privacy, traceability and cyber-evidence.

3. SPECIFIC COURSE/STUDENT LEARNING OBJECTIVES:

The course is aimed at imparting knowledge and skill sets required to assume the overall responsibilities of administration and management of the security of an enterprise information system. After completing the course, students will be able to:

- Carry out a detailed analysis of enterprise information security by performing various types of analysis such as vulnerability analysis, penetration testing, audit trail analysis, system and network monitoring,
- Carry out detailed risk analysis and assessment of enterprise information systems using various practical tools and techniques.
- Design detailed enterprise-wide security plans and policies; deploy appropriate safeguards at all the levels in the organization by providing due consideration to the life cycle of the enterprise information systems and networks, as well as its legal and social environment.
- Identify and prioritize information assets
- Identify and prioritize threats to information assets
- Define an information security strategy
- Plan for and respond to intruders in an information system
- Describe legal and public relations implications of security and privacy issues
- Present a disaster recovery plan for recovery of information assets after an incident

Student Learning Outcomes (SLO's)

As a result of completing this course, students will be able to:

- Demonstrate an understanding of the differences between various forms of computer and information security threats where they arise, and the appropriate management tools to respond to them;
- Demonstrate an appreciation of some common security pitfalls;
- Show knowledge of the techniques used to quantify the costs of cybersecurity and information breaches;
- Describe threats to information security;
- Identify methods, tools and techniques for combating external and internal threats and vulnerabilities to data assets in the enterprise;
- Identify types of attacks and problems that occur when systems are not properly protected;
- Explain integral parts of overall good information security practices;
- Identify and discuss issues related to access control;
- Describe the need for and development of information security policies, and identify guidelines

- and models for writing policies;
- Define and perform risk management and explain why it is an important component of an information security strategy and practice;
- Describe the types of contingency plans and the steps involved in developing each;
- Identify security issues related to personnel decisions, and qualifications of cybersecurity;
- Evaluate, mitigate or eliminate all areas of information security weakness in the enterprise
- Identify the requirements to secure the physical perimeter information center of an enterprise;
- Develop a comprehensive security assessment for an existing enterprise information infrastructure;
- Overall, recommend mitigations to protect digital assets in the enterprise;
- Manage cybersecurity disaster recovery incident handling, cybersecurity policy implementation, and the application of relevant laws to cybersecurity in the enterprise.

4. REQUIRED TEXTBOOK

There is no one textbook that covers all the topics considered in this course. The following is the primary textbook for the course:

- *Management of Information Security*, M.E. Whitman, H.J Mattord

Other Textbook References and Resources:

- Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*
- Micki Krause, Harold F. Tipton, *Handbook of Information Security Management*
- *Guide to Disaster Recovery*, M. Erbschilde
- *Guide to Network Defense and Countermeasures*, G. Holden
- *Computer Security: Art and Science*, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2003 (Available online for Pitt Students)
- *Security in Computing*, 2nd Edition, Charles P. Pfleeger, Prentice Hall
- *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson, Wiley, John & Sons, Incorporated 2001
- *Software Security: Building Security In* (by Gary McGraw)
- *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities* (by Mark Dowd, John McDonald, Justin Schuh)

Additional reading list of journals and articles and NIST/GAO and federal reports.

Internet Resources:

- NIST publications (<http://csrc.nist.gov/publications/nistpubs/index.html>)
- SP 800-12 An Introduction to Computer Security: The NIST Handbook (HTML (<http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html>) or 1.7 MB PDF (<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>))
- SP 800-26 Security Self-Assessment Guide for Information Technology Systems (1.5 MB PDF (<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>) or 922 kb Word Doc (<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.doc>))
- SP 800-30 Risk Management Guide for Information Technology Systems (480 kb PDF (<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>))
- SP 800-34 Contingency Planning Guide for Information Technology Systems (1.9 MB PDF (<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>))

- Volunteer Leader Recognition in support of SHRM and the HR Profession (Given 2015-2018)
- Who's Who in Science and Engineering 12th – 2016 edition
- Center for Scholastic Inquiry (CSI) – Best Paper in Business Track Award (Oct. 1, 2014)
- FBI Citizens Academy 2014 Top Gun Award
- New Faculty of the Year Award (UOG-May 2014)
- Who's Who in America 68th (2014 ed), 69th (2015 ed) and 70th (2016 Platinum ed)
- 60th Anniversary, University of Guam - Featured Alumni Triton Success Story
- Magna Cum Laude (Bachelor Degree)
- University of Guam's College of Business and Public Administration Dean's Outstanding Graduate Award for Fall 2001
- University of Guam's Regent's List (99/SP, 99/FA, 00/SP, 00/FA, 01/SP, 01/FA)
- University of Guam's President's List (98/FA, 99/FA, 01/SP)
- University of Guam's Dean's List (99/SP, 00/SP, 00/FA, 01/FA)
- Datatel Scholarship Recipient
- Merit Scholarship Recipient
- National Dean's List (98-99/99-00/00-01)
- National Dean's List Multiple Year Award Recognition
- 2001 Leonard R. Brice SPHR Undergraduate Leadership Award Nominee
- 28th Guam Legislature Official Commendation and Congratulations for inclusion in Who's Who in American Colleges and Universities (Executive Committee Certificate No.42)
- 26th Guam Legislature Official Commendation and Congratulations for inclusion in Who's Who in American Colleges and Universities (Legislative Certificate No.1)
- 26th Guam Legislature Official Commendation and Congratulations for inclusion in Who's Who in American Colleges and Universities (Legislative Certificate No.53)
- 26th Guam Legislature Office of the Speaker Antonio R. Unpingco Official Commendation and Congratulations for inclusion in Who's Who in American Colleges and Universities (Ltr. Dated May 4, 2001)
- Who's Who in American Colleges and Universities (00, 02 & 05)
- National Collegiate Business Merit Award Winner
- United States National Collegiate Award Winner
- United States All-American Scholar
- United States Achievement Academy Member
- 26th Guam Legislature Official Commendation and Congratulations for outstanding service in production of "I Lihenden Duhendes" (Legislative Certificate No.26-003)
- Official Commendation and Recognition by UOG Endowment Foundation for support and outstanding service for participation and coordination of the Student Support Committee for "I Lihenden Duhendes" UOG Spring Musical 2001

PROFESSIONAL CREDENTIALS

- L5 Behavioral Governance – certified by 3Ethos with the L5 professional designation (Nov. 2018)
- AIF: Accredited Investment Fiduciary – Certified January 2018 by Fi360
- CFE: Certified Fraud Examiner – Certified June 2016 by the Association of Certified Fraud Examiners
- SPHRi: Senior Professional in Human Resource – International / rebranded and renamed from the HRMP™ - Certified by HRCI (Feb. 2016)
- CFD: LERN Certified Faculty Developer – Certified by Certified Faculty Development Institute - May 2015
- SHRM-SCP: SHRM Senior Certified Professional – January 2015
- HRMP: Guam's 1st Human Resource Management Professional – Certified by HRCI (2013)
- PHR: Professional in Human Resources – Certified by HRCI (2012)
- CM - One of Guam's first Certified Managers – Credentialed in 2011 by Institute of Certified Professional Managers /James Madison University College of Business
- KHS: Equestrian Order of Holy Sepulchre of Jerusalem – Chivalrous Order of Knighthood (2012-Present)
 - Instrumental in establishing this Order with roots in the First Crusade (c1099)
 - Appointed Founding Chancellor of the Council of the Magistral Delegation of Guam
- KSS: Equestrian Order of St. Sylvester Pope & Martyr – Pontifical Order of Knighthood conferred by Pope Benedict XVI (2009)

PROFESSIONAL MEMBERSHIPS, BOARDS, AND AFFILIATIONS

- Founding member of the UOG Phi Kappa Phi Honor Society (official induction pending - 2019)
- Epsilon Pi Phi Emergency Management Honor Society founding Advisor (Aug. 2019)
- Omicron Delta Epsilon (ODE) International Honor Society for Economics Member (inducted May 2019)
- Executive Order 2019-04: Appointed Vice-Chair to the Governor's Task Force to Reform Government Permitting Procedures (February 2019 – August 2019)
- Member, Behavioral Governance Society-3Ethos (November 2018-Present)
- Dulce Nombre de Maria Cathedral-Basilica Parish Finance Council (November 2018-Present)
- GPD Honorary Deputy Chief of Police (Sworn in August 7, 2018)
- FBI Guam Citizens Academy Alumni Association (November 20, 2015 – Present)
 - Founding Board Member and Inaugural Board VP (2015-Present)
 - Federal Bureau of Investigations (FBI) Citizens' Academy Graduate - Alumni since 2012
 - Top Gun Award (2014)
- SHRM Guam Board of Directors Student Relations Director (2015-2018)
 - SHRM 100% Chapter
 - 2018 Top 25 Fundraising Chapter
 - 2017 SHRM Excel Platinum Chapter Award
 - 2017 Pinnacle Award Chapter - the highest honor given to SHRM state councils and chapters for notable contributions to the human resource profession. Main Award Packet Co-Author.
 - 2017 Top 25 Fundraising Chapter SHRM Foundation
 - 2017 Learning System Champion
 - SHRM Foundation 2016 Chapter Champion
 - 2016 SHRM Excel Platinum Chapter Award
 - 2016 Top 25 Fundraising Chapter SHRM Foundation
 - 2016 SHRM Learning System Champion
- Rotary E-Club of Pago Bay Guam Member – chartered June 12, 2014 (2014-Present)
 - President (2019-2020)
 - Secretary (December 2014-2016)
 - Inaugural Int'l. and Community Service Director and Charter Member (June 2014 – March 2015)
- Fiduciary Academy Member (2018-Present)
- Golden Key International Honor Society (inducted 2018)
- Sigma Beta Delta International Honor Society for Business, Mngt. and Admin. (inducted Nov. 2017)
- Alpha Phi Sigma Criminal Justice Honor Soc. Lambda Psi Chapter – Honorary Member (inducted April 2017)
- Institute of Certified Professional Managers (ICPM) Exam Advisor (2012-2017)
- Techstar Community Leader (2016-present)
- Blue Key Honor Society (inducted 2016)
- Capella University Peer Mentor (2012-2016)
- Imagine Guam Core Steering/Facilitation Committee – Appointed by Governor of Guam (2015)
 - Imagine Guam Values Committee Facilitator
 - Imagine Guam Convention I, II, III Imagination Team Facilitator
 - Imagine Guam Planning Team – Workforce Rehabilitation Lead
- Academy of Criminal Justice Sciences Member (ACJS) – (2015 – 2017)
- Pi Alpha Alpha Global Honor Society for Public Affairs and Administration (inducted 2015)
- Association of Certified Fraud Examiners Member (ACFE) – (Feb 2014 – Present)
- Guam Hotel and Restaurant Association Member (2013-Present)
- Institute of Certified Professional Managers (ICPM) International Advisory Group (IAG) Founding Member (2013-2014)
- Institute of Certified Professional Managers (ICPM) Exam Advisor (2012-2017)
- KHS: Equestrian Order of Holy Sepulchre of Jerusalem – Chivalrous Order of Knighthood (2012-Present)
 - Instrumental in establishing this Order with roots in the First Crusade (c1099)
 - Appointed Founding Chancellor of the Council of the Magistral Delegation of Guam
- Catholic Cemeteries of Guam, Inc. Founding Board of Directors (2011-2014)
- Capella University Ambassador (2011-2014)

- Association for Psychological Type International – APTi (Since 2010-Lifetime Member)
- Society for Human Resource Management (1998-Present)
- Catholic Cemetery Conference Member (2002–2012)
- Chi Omicron Gamma Honor Society (inducted 2001)
- National Catholic Education Association Teacher Associate (2000 & 2001)
- President, Collegiate Chapter of the Society for Human Resource Management (2000-2001)
- University of Guam Student Government Public Relations Committee Member (2000-2001)
- Island Wide Guam Job Fair Planning Committee (2000)
- Guam Business Show coordinator for jobsonguam.com/SHRM Booth (2000)
- National Honor Society President and National Junior Honor Society President

PROFESSIONAL CERTIFICATIONS AND TRAINING

- Selected for the invitation only 2019 NASPAA Next Class – How to prepare for the NEXT 50 years of Public Affairs Education (Oct. 2019)
- First Certified Manager (CM) Certified Instructor and CM Exam Proctor (Aug. 2019 – Present)
- Rotary International District 2750 2019 President-Elect Training Seminar (May 2019)
- IACBE Accreditation Institute (April 2018 and 2019)
- SHRM Foundation’s Veterans at Work Certificate (Feb. 2019)
- Fiduciary Essential (FE®) Certificate Training – Fi360 (Nov. 2018)
- Initial Law Enforcement Response to Suicide Bombing Attacks (ILERSBA) Mobile Course (Nov. 2017) - New Mexico Tech in partnership with Guam Homeland Security
- Understanding and Planning for School Bomb Incidents (UPSBI) Mobile Course (Nov. 2017) - New Mexico Tech in partnership with Guam Homeland Security
- EEOC Guam Technical Assistance Seminar 2017 – EEOC Training Institute (Sept. 2017)
- Non-Confrontational Interview & Interrogation - Wicklander-Zulawski & Associates, Inc. (August 2017)
- FBI National Improvised Explosives Familiarization and Chemical Industry Outreach Workshop (April 2017)
- Incident Response to Terrorist Bombings (IRTB) – New Mexico Tech/EMRTC First Responder Training Program (March 2017)
- FEMA Emergency Management Institute (EMI) - National Incident Management System (NIMS)
 - IS-100.b - Introduction to Incident Command System ICS-100 (March 2017)
 - IS-100.c – Introduction to the Incident Command System ICS-100 (June 2019)
 - IS-100.he - Introduction to the Incident Command System ICS-100 for Higher Education (March 2017)
 - IS-200.b - ICS for Single Resources and Initial Action Incident, ICS-200 (March 2017)
 - IS-230.d - Fundamentals of Emergency Management (June 2019)
 - IS-240.b - Leadership and Influence (June 2019)
 - IS-700.a - National Incident Management System (NIMS) An Introduction (March 2017)
 - IS-702.a - NIMS Public Information (June 2019)
 - IS-703.a - NIMS Resource Management (June 2019)
 - IS-706 - NIMS Intrastate Mutual Aid – An introduction (June 2019)
 - IS-00800.b - National Response Framework, An Introduction (March 2017)
- Guam Joint Criminal-Epidemiological Investigations Workshop (Feb. 2017) – FBI and CDC
- Criminal Justice and Juvenile Justice Evaluation Training – Univ. of Cincinnati Corrections Inst. (Dec. 2016)
- Type Coaching Using Multiple Models – Practitioner Certified by APTi (August 2016)
- The Justice System and Persons with Disabilities Training– Judiciary of Guam (2016)
- Explosive Response Training – Guam FBI (2016)
- National Criminal Justice Association Grants Management Workshop Training (2015)
- One Community Guam: Engaging Our Community in Crime Prevention, Strengthening Protections for Vulnerable Populations, and Reentry Efforts through Workforce Development Strategies Training – U.S. Attorney’s Office (2015)
- Educating, Retaining, and Graduating First Generation Students - Souder, Betances & Assoc. (2015)
- TIPS® (Training for Intervention Procedures) Trainer - Certified September 2015

- Entrepreneurial Mindset Profile (EMP) Certified - Certified in December 2014 by the Institute Leadership Development Institute at Eckerd College (a Network Associate of the Center for Creative Leadership) and named a Founding Practitioner
- Ethics in Government Train the Trainer Qualifier (4 GCA 15410) - Certified by UOG SBPA (2014)
- Universal HR Management Strategies SHRM Learning System (2013)
- Project Management Preparation Course – Leading Edge (2013)
- FBI Citizens' Academy Graduate - Federal Bureau of Investigations (2012)
- University of Maryland University College - Online teaching certified (2012)
- Graphology Training - Lisa Schuetz (Taken over 15 courses between 2011 and 2012)
- Leadership Process: Motivating Achievement - Spencer-Shenk-Capers & Assoc., Inc. (2012)
- Founding Board Treasurer of St. Thomas Aquinas Catholic High School (2008-2012)
- Introduction to Body Language and Type: Reading People (APti): (2011)
- Guam's 1st Strong Interest Inventory® (Strong) – Certified in 2011 by GS Consultants
- Guam's 1st and only Certified MBTI® (Myers-Briggs Type Indicator) Master Practitioner (2011)
- MBTI® - Myers-Briggs Type Indicator Assessment – STEP I, II, & III Certified
 - Guam's First and only Step III Certified Practitioner
 - MBTI™ Step III: Certified by Center for the Application of Psychological Type (CAPT) – 2011 - developed a "Perception and Judgment Model" for use in certification and training
 - MBTI™ Step I & II: Certified by Center for the Application of Psychological Type (CAPT) –2009
 - Type Coaching Executives and Managers Certification Workshop: Fairfax, VA - 2011
 - Generations and Type Training Certification Workshop: Fairfax, VA - 2011
 - Using Type with Leaders and Managers Certification Workshop: Fairfax, VA - 2011
 - Type and Temperaments Certification Workshop: Fairfax, VA - 2011
 - MBTI/Type Trainers Workshop: Fairfax, VA - 2011
- Klein Group Instrument® (KGI) – Certified in 2011 by Otto Kroger & Associates (OKA)
- Pearson-Marr Archetype Indicator® (PMAI) – Certified in 2011 by Otto Kroger & Associates (OKA)
- Portraits of Jung Type Behavior™ (JTB)– Certified in 2011 by Otto Kroger & Associates (OKA)
- Fundamental Interpersonal Relations Orientation (FIRO-B® and FIRO Business®) assessments – Qualified in 2011 by CPP
- Murphy-Meisgeiger Type Indicator for Children® (MMTIC): Qualified in 2011/certified in 2014 by CPP
- Thomas-Kilmann Conflict Mode Instrument (TKI) – Qualified in 2011 by CPP
- Collaborative Institutional Training Initiative (CITI): Protection of Human Research Subjects (2010)
- EQ-i® and EQ-i 2.0® - Emotional Quotient Index – Certified in 2009 by Multi-Health Systems (MHS) and among Guam's first certified emotional intelligence practitioners
- Founding Member of the International Center for Holy Relics, Inc. (2009)
- Certificate, International Human Resource Management Seminar (2003)
- Certificate, EEOC: Affirmative Action Conference (2001)
- Certificate, EEOC: Basic and Advanced EEO Topics, Technical Assistance Program Seminar (2000)

PROFESSIONAL EXPERIENCE

President/Senior Consultant, Allied Business Consultants, Inc., GU 2017-Present
 Development Consultants that combine the most experienced, credentialed, and dynamic talent this side of the Western Pacific to offer a wide range of services. Clients include local and regional governments, military, nonprofits, private companies (small, family-owned to corporate), medical, construction, educational institutions, etc. <http://www.alliedbusinessglobal.com/>

Director & Co-Founder, UOG Regional Center for Public Policy, GU 2016-Present
 The Regional Center for Public Policy (RCPP) was created to be a regional nexus in Micronesia where leaders converge to address, research, collaborate and solve crucial issues in relation governance, leadership and public policy. RCPP creates globally minded and locally relevant strategic conduits by leveraging a symbiotic

and complementary synergy between the university community, public-private partnerships, public service collaborations, SBPA programs/partners and others.

Consultant, Leading Edge, GU **2014-Present**

Business Consultants that offer a myriad of services, with a proven track record, for non-profit and military sectors throughout the Western Pacific and Asia.

Owner, J|Rivera Consulting, GU **2011-Present**

Started in 2011 to provide clients with dynamic Educational, Executive, Leadership, Organizational Training, Development and other related consulting services; backed by the most prominent developmental assessments of the day.

Consultant, Area Defense Counsel Anderson, AFB, Guam **2013**

Provided consulting and served as an expert witness for the Area Defense Counsel.

Practicum Counselor, ISA Psychological Services, GU **2012-2013**

Isa Psychological Services Center is a University of Guam sponsored training clinic that offers a variety of free professional services to the University of Guam's students, faculty, staff and the greater community.

Owner, the Source, GU **2004-Present**

Started in 2004, "the Source" was created as an outsourcing company for various types of products, gift related items, souvenirs, and pre-paid cards.

Executive Director, Archdiocesan Development Group (ADG), GU **2008-2014**

Promoted to lead and consolidate specific institutional and functional activities of the Archdiocese of Agaña. The ADG was created to streamline and strategically align critical management talent, effectively administer debt management, and anticipate growth capacity.

- Created the concept, organizational, and formal structure of the ADG.
- Responsible for the following institutions:
 - Guam Catholic Television
 - Exploratory team for the first Archdiocesan Television Station/Channel
 - U Matuna Si Yu'os (formally Pacific Voice) – Roman Catholic Newspaper of the Archdiocese of Agaña (2011-2013)
 - Facilitated and assisted in the takeover, restructuring and redesign of the newspaper
 - Reinstated the original Chamorro name of the publication - U Matuna Si Yu'os
 - Founding member of St. Thomas Aquinas Catholic High School (2008-2012)
 - 1st Catholic High School in 40 yrs.
 - Founding Board Treasurer (2008-2012)
 - In the Founding Year
 - Received WASC accreditation in founding year
 - Over 83% of the student body made "Honor Roll" In the first quarter of 2008-2009.
 - 100% passing rate on AP exams with 40% achieving a perfect score of 5.
 - Carmel on the Hill Archdiocesan Retreat Center (2010-2012)
 - Conversion of a Carmelite Monetary into an Archdiocesan Retreat Center
 - Largest retreat center on the island with capacity for several hundred retreatants
 - Coordinated local and regional events for the facility
 - Created the marketing, branding, business plan, etc.
 - Cathedral-Basilica Gift Shop
 - Started the gift shop in 1999
 - Facilitated buyout and merger with John Paul the Great Catholic Book Store
 - Grew to the largest and most complete religious (Catholic Store) on Guam
 - Catholic Cemeteries of the Archdiocese of Agaña
 - Catholic Cemeteries of Guam, Inc. founding Board of Directors (2011-2014)

- See entries under Catholic Cemeteries below
- Cathedral-Basilica Media Ministries
 - Graphics Design, Videography, Still Photography, Editing, Scripting, Commercial production, Audio, Internet Streaming
 - Internet streaming and Cable TV airing of various Liturgical Events
 - Operate NewTek TriCaster System
- National Museum of the Dulce Nombre de Maria Cathedral-Basilica
- Dulce Nombre de Maria Cathedral-Basilica
 - Founding Member of the International Center for Holy Relics, Inc. (2009)
 - Coordinated the production of "The Golden Harvest Documentary" (2008) and "Servus Tuus Documentary" (2009)
 - Archdiocesan Logistics Coordinator for "Operation Special Intention" Military Relic Tour (Guam-2009); the Pilgrim Relics of St. Therese of Lisieux (Guam, Saipan, Tinian, Rota-2008/Guam-2003); Relics of the Passion Tour (Manila, Philippines-2008); and Relics of the Passion Tour (Guam-2007)
 - Executive Planning Committee for the 50th Anniversary – the Golden Jubilee of the Dulce Nombre de Maria Cathedral-Basilica (2008)
 - Executive Planning Committee for the Monsignori Elevation (2006).
 - Official Delegation to Lisieux (France) to return the Pilgrim Relics of St. Therese of Lisieux
 - Archdiocesan Executive Committee for the Great Jubilee of 2000
 - Post Beatification - Blessed Pedro Calungsod Planning Committee
 - Instituted the Logo / Branding for the Cathedral-Basilica
- Responsibilities include Hosting of Vatican Officials and Church Dignitaries; Coordination of island-wide liturgical events, development activities, documentaries, concerts, gallery exhibits, fundraising events, etc.

Executive Director, Catholic Cemeteries of the Archdiocese of Agaña, GU 2007-2008

Responsible for three Archdiocesan Catholic Cemeteries with over half a million in sales and 20M in assets (Pigo Catholic Cemetery, Anigua / Holy Cross Catholic Cemetery, Yona / Mt. Carmel Catholic Cemetery, Agat)

- Complete reorganization, strategic/personnel realignment, and business model overhaul
- Responsible for the following other institutions:
 - Carmel on the Hill Archdiocesan Retreat Center
 - National Museum of the Dulce Nombre de Maria Cathedral-Basilica
 - Cathedral-Basilica Gift Shop (largest religious store on Guam)
 - Cathedral-Basilica Media Ministries (Graphics Design, Videography, Still Photography, Editing, Commercial production, Audio, Internet Streaming)

Executive Director of Administration and Finance, Catholic Cemeteries, GU 2006-2007

Established and managed critical organizational and formal structures; led the financial management, stabilization of revenues, debt service, and human resource matters.

- Responsible for all personnel, finance and human resources matters
- Established SOPs, handbook, wage scale, position descriptions and formal organizational chart
- Established 401K, medical/dental Benefits and performance appraisals
- Managed the debt service that was used to rehabilitate existing facilities, beautify grounds, construct new buildings and increase inventory

Sales and Marketing Manager, Catholic Cemeteries, GU 2001-2006

Established and managed the first sales and marketing department. Recruited, trained and supervised all independent sales counselors and created all program materials; Implemented marketing campaigns, educational and incentive programs to fuel and further business development.

- Led financial turnaround from negative to positive cash flow and financial sustainability
- Increased market share from 6% to 18%
- Designed and crafted all graphic concepts, layout, designs, placement
- Responsible for the Cathedral-Basilica Gift Shop
- Assisted with the National Museum of the Dulce Nombre de Maria Cathedral-Basilica

Business Startup, Cathedral-Basilica Gift Shop, GU **1999-2014**

Established and managed the all aspects of the religious retail shop startup.

- General Manager during its initial years realizing exponential growth in the first 3 years
- Facilitated buyout and merger with John Paul the Great Catholic Book Store to become the largest and most complete religious store on the island
- Created the Catholic Education Series and other initiatives

Part Owner, Brown Bag Café, Eastwood, Philippines **2005-2007****Administrative Assistant, Dulce Nombre de Maria Cathedral-Basilica, GU** **1994-2001**

- Assistant Curator - Monsignor Oscar Calvo Gallery (1997-2001)
- Archdiocesan Executive Committee for the Great Jubilee of 2000
- Post Beatification – Blessed Pedro Calungsod Planning Committee
- Dulce Nombre de Maria Cathedral-Basilica Restoration and Rededication Committee
- Confirmation Retreat Master and Facilitator
- Served on numerous fundraising committees, planning committees, and coordination of island-wide archdiocesan events.

OTHER VOLUNTEER/COMMUNITY SERVICE

- Reverence: Choir – (2001 – Present)
 - Dulce Nombre de Maria Cathedral-Basilica 7:00pm Choir (2001-May 2014)
 - Contributing composer of "Mass of Peaceful Reverence" (2007)
- Emmaus Choir - Dulce Nombre de Maria Cathedral-Basilica 11:30am Choir (1998-2003)
- Choir - Blessed Diego, Tumon Catholic Church (1999-2001)
- Confraternity of Christian Doctrine Teacher: Nuestra Senora de las Aguas - Guam (1997-1999)
 - 6th Grade and Confirmation teacher
 - Formed Confirmation Youth Choir

REFERENCES

Available upon request

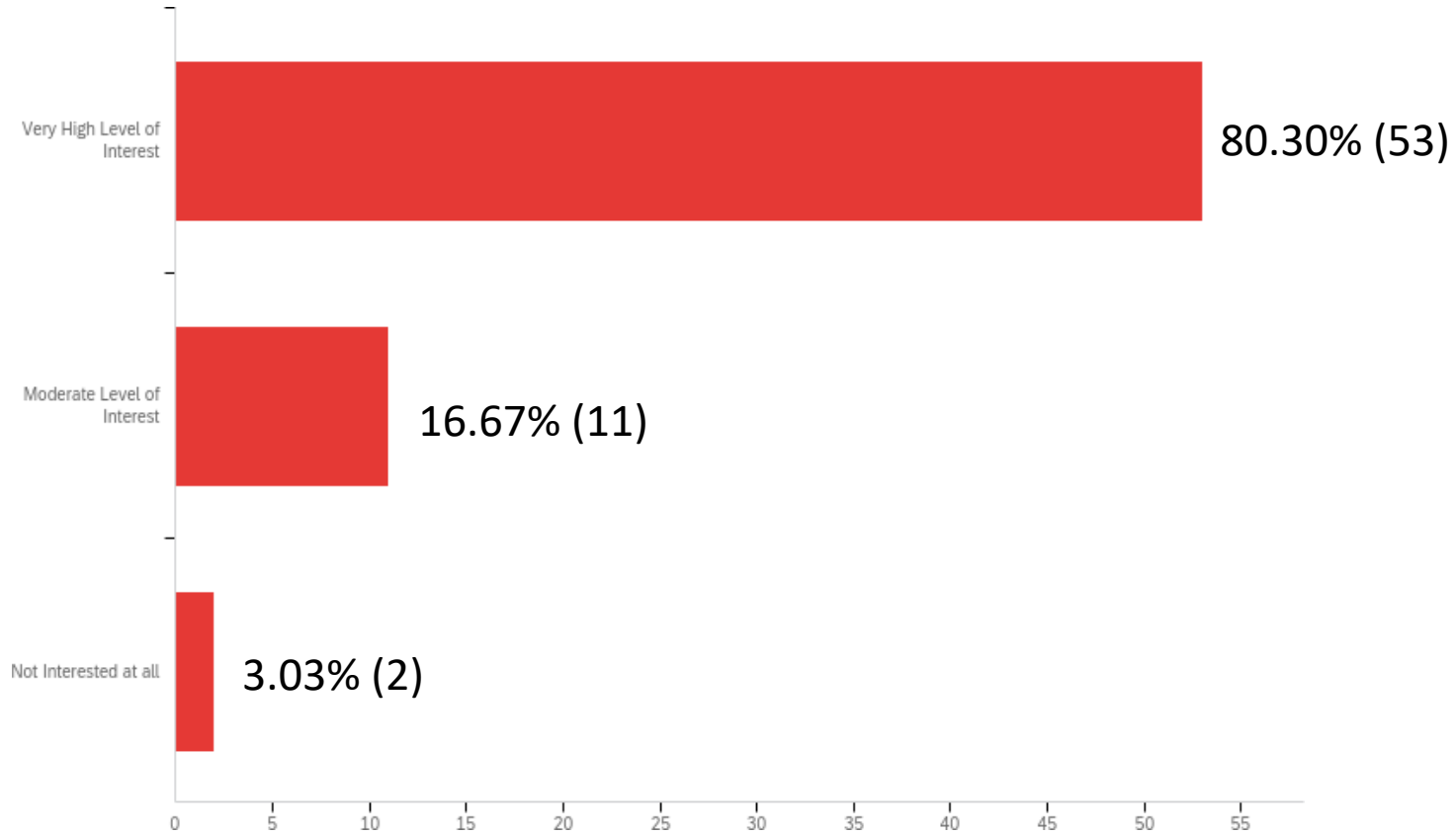
**Survey Report of Stakeholder Interest
and Support for the
Minor in Cybersecurity Management and a
Professional Certificate Program
in Cybersecurity Management**

**SCHOOL OF BUSINESS AND PUBLIC ADMINISTRATION
UNIVERSITY OF GUAM
DECEMBER, 2019**

Cyber-Security Management Minor and
Professional Certificate Program in
Cyber-Security Management
Program Demand Report

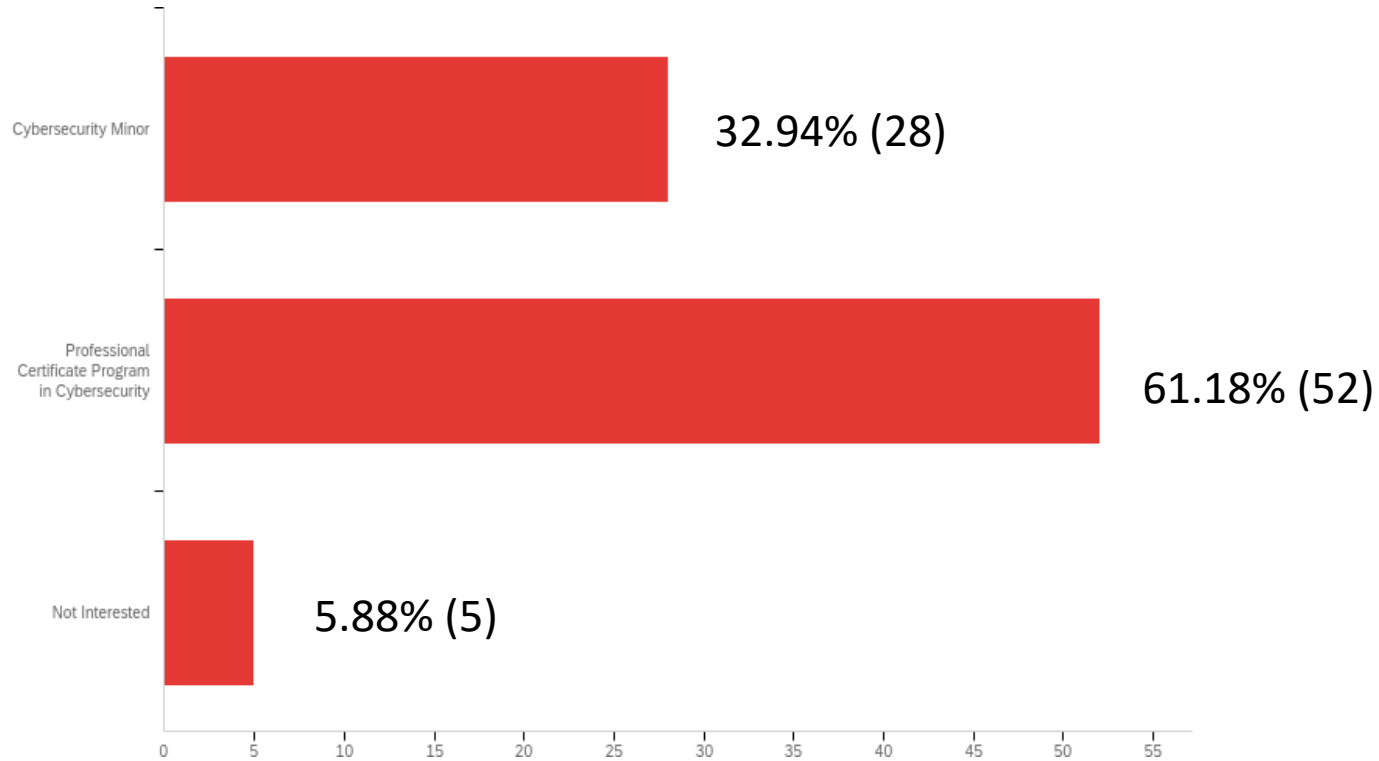
April 6th 2020, 5:46 pm MDT

1. Can you tell us your level of interest and support for the offering of the proposed SBPA Cybersecurity Management and Professional Certificate Program in Cybersecurity Management: (N=66)

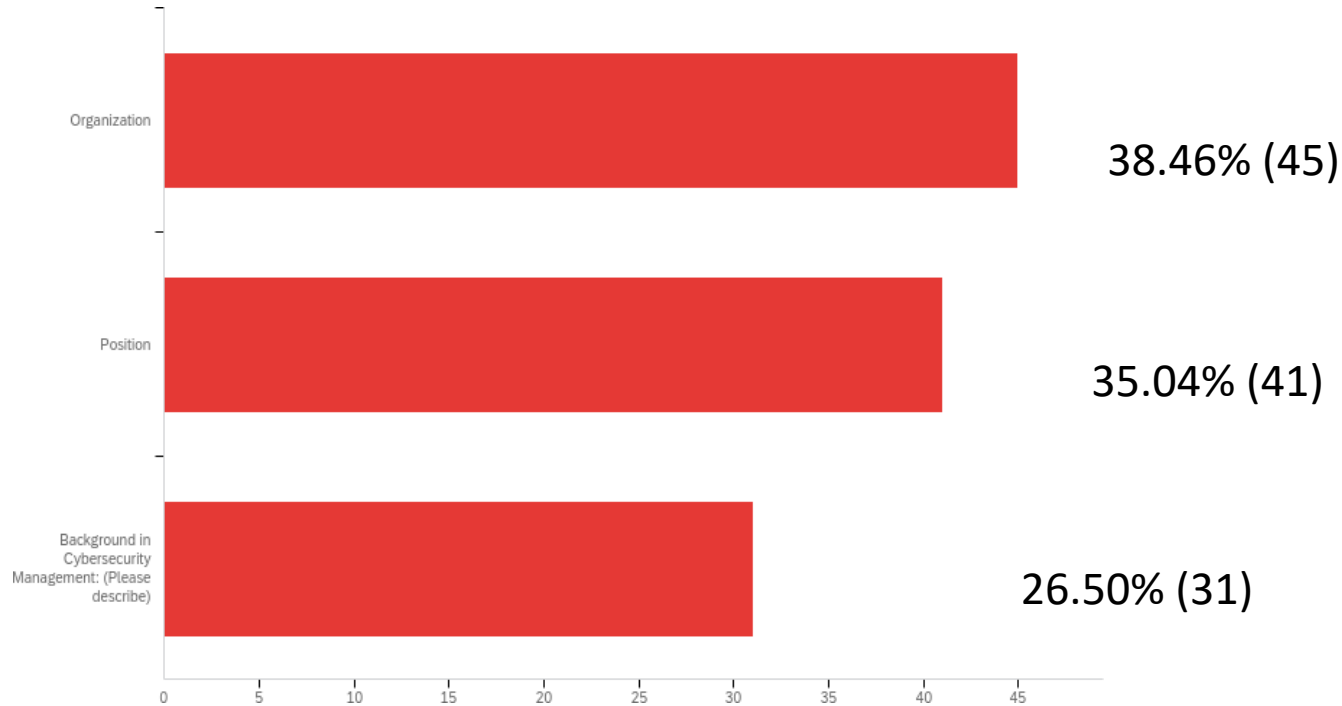


| Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---------|---------|------|---------------|----------|-------|
| 1.00 | 3.00 | 1.23 | 0.49 | 0.24 | 66 |

2. Would you be interested enrolling in the Cybersecurity Minor or the Professional Certificate Program in Cybersecurity Management? N=85



3. If you are a working professional, can you tell us about your organization and your current role, as well as any background you may have in Cybersecurity Management: N=117



4. If you are a working professional, can you tell us about your organization and your current role, as well as any background you may have in Cybersecurity Management:

| 4A. Organization | | |
|--|---|---|
| Department of Agriculture | Guam Homeland Security/Mariana Regional Fusion Center (2) | Guam Power Authority (3) |
| HRRA | | Government Entity. Housing and Finance of Housing |
| Self employed | Sheraton Hotel | |
| Department of Education | USCBP | Guam Economic Development Authority |
| Government of Guam (4) | University of Glasgow | DPW |
| | Nisga'a Data System | ZAN Administrative Services |
| Guam Police Department (4) | US ARMY | |
| Guam Fire Department | PIC Hotel | Simon Sanchez High School |
| | Guam Surgicenter | Pacific Data Systems |
| University of Guam (6): CNAS CE&O; OIT | Guam Community College | Pacific Human Resource Services |
| | Guam Air National Guard | Guam Veterans Affairs Office |

4. If you are a working professional, can you tell us about your organization and your current role, as well as any background you may have in Cybersecurity Management:

| 4B. Position | | \ |
|---------------------------------------|--|--|
| Executive Housekeeper | President | Assistant General Manager, Engineering & Technical Services |
| Extension Associate | Teacher (2) | |
| Police Major | Administrative Manager | Agency head |
| Police Officer III (2) | Intel Analyst | Director |
| PhD researcher | Telecommunication/Broadband /Cyber Security | Mayor |
| Cybersecurity Engineer | | Records & Registration Tech |
| IT Manager | Field IT | Jr. Information Security Analyst |
| CEO | Conservation Officer | Information Security Analyst |
| Instructor | Fire lieutenant fire instructor | Captain |
| Administrative Services Supervisor | Extension Assistant | Manager, Power System Control Center |
| | Program Manager | |
| Land Agent II | Jr. Network Engineer | CITO |

| | |
|------------------------|---------------------|
| Conservation Officer I | Intel Analyst-Cyber |
| Planner III | Shareholder |

4. If you are a working professional, can you tell us about your organization and your current role, as well as any background you may have in Cybersecurity Management:

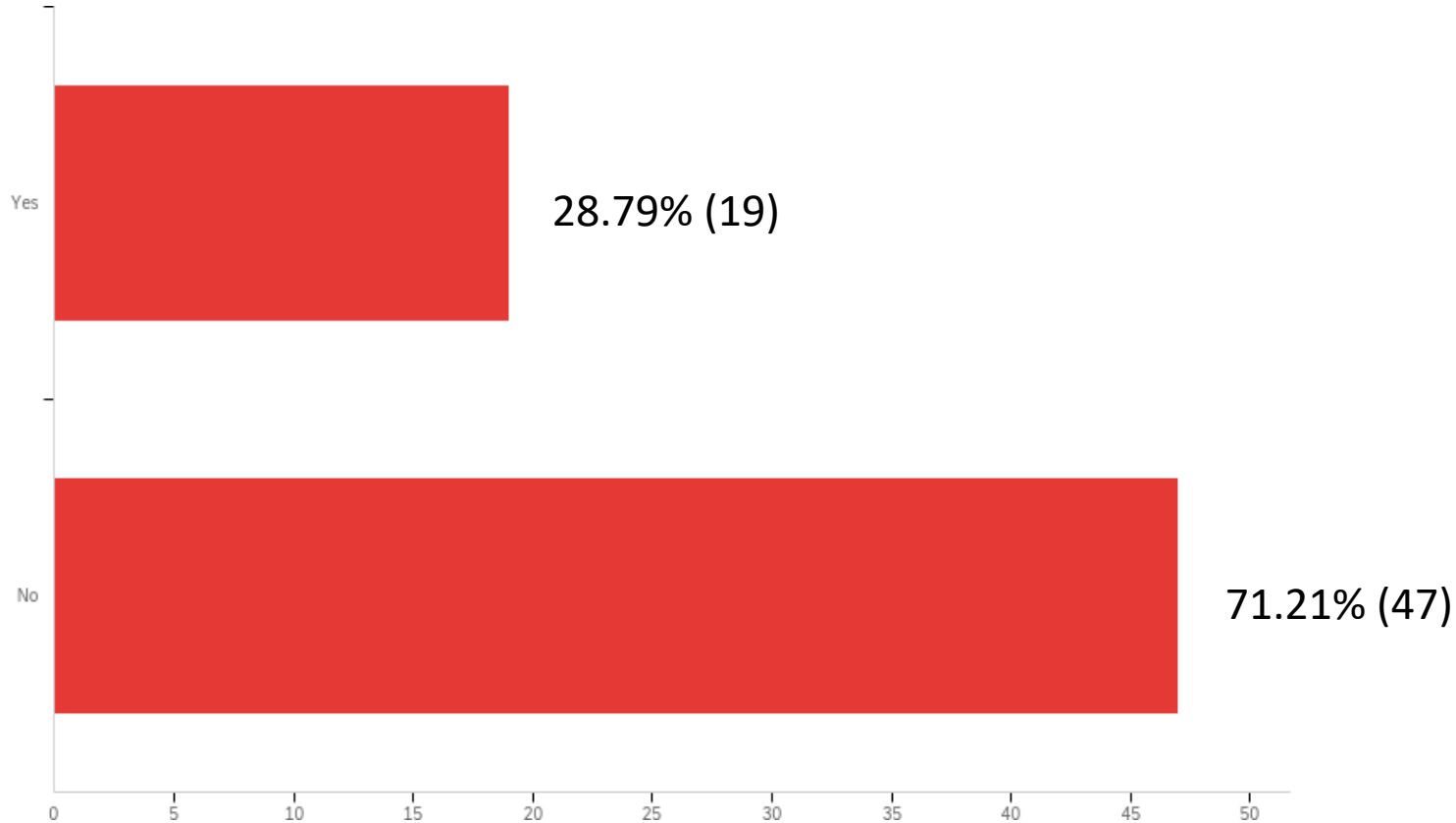
| 4C. Background in Cybersecurity Management: (Please describe) | | |
|---|---|---|
| | None, but my research is in CSR in the tech sector | Undergraduate Certificate in Cybersecurity |
| Prior basic military end-user training certificate, self-training on CISSP and article research | 3.5 years working with air force to ensure compliance of dod level cybersecurity requirements | I have attended seminars in the US on ICS (industrial control systems)and protecting them from cyber attacks. We have studied the cyber attacks of the Ukraine and other utilities. We also follow NIST 800 and other NERC standards to help prevent cyber attacks. |
| None. No background (8) | Self Research | |
| Not much | Hands on learning to meet regulatory requirements | |
| Some | Project Foresight | |
| Network Security Best Practices | Accounting Software Security, Bank ACH/Wire Security, Payroll Transmittals | |
| Basic | IT Project Manager role. Information security, along with cyber security are very relevant. | CISA AND GICSP CERTIFIED |
| When at Homeland Security, I organized a Cyber Security Committee | | Helped form GPA's Cyber Security Management. Cornerstone of GPA's Smart Grid ARRA Grant Project |
| Management of GPD | | Law Enforcement and Homeland Security education, training and |

Information Technology
Section

Intel Analyst

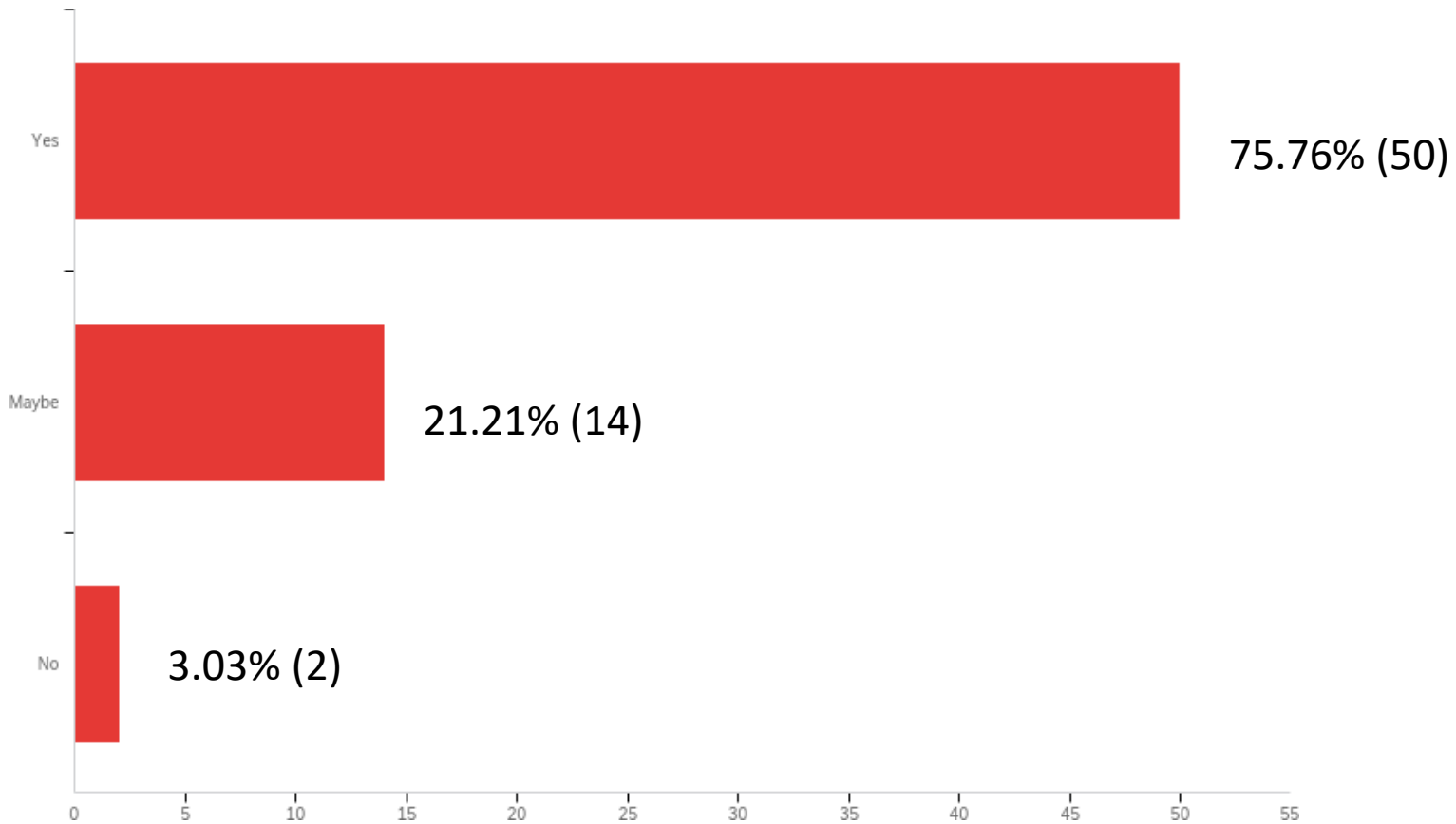
experience in cyber crime and
cyber terrorism issues.

5. Does your organization currently offer Cybersecurity Management education or training opportunities that you can participate in? N=66



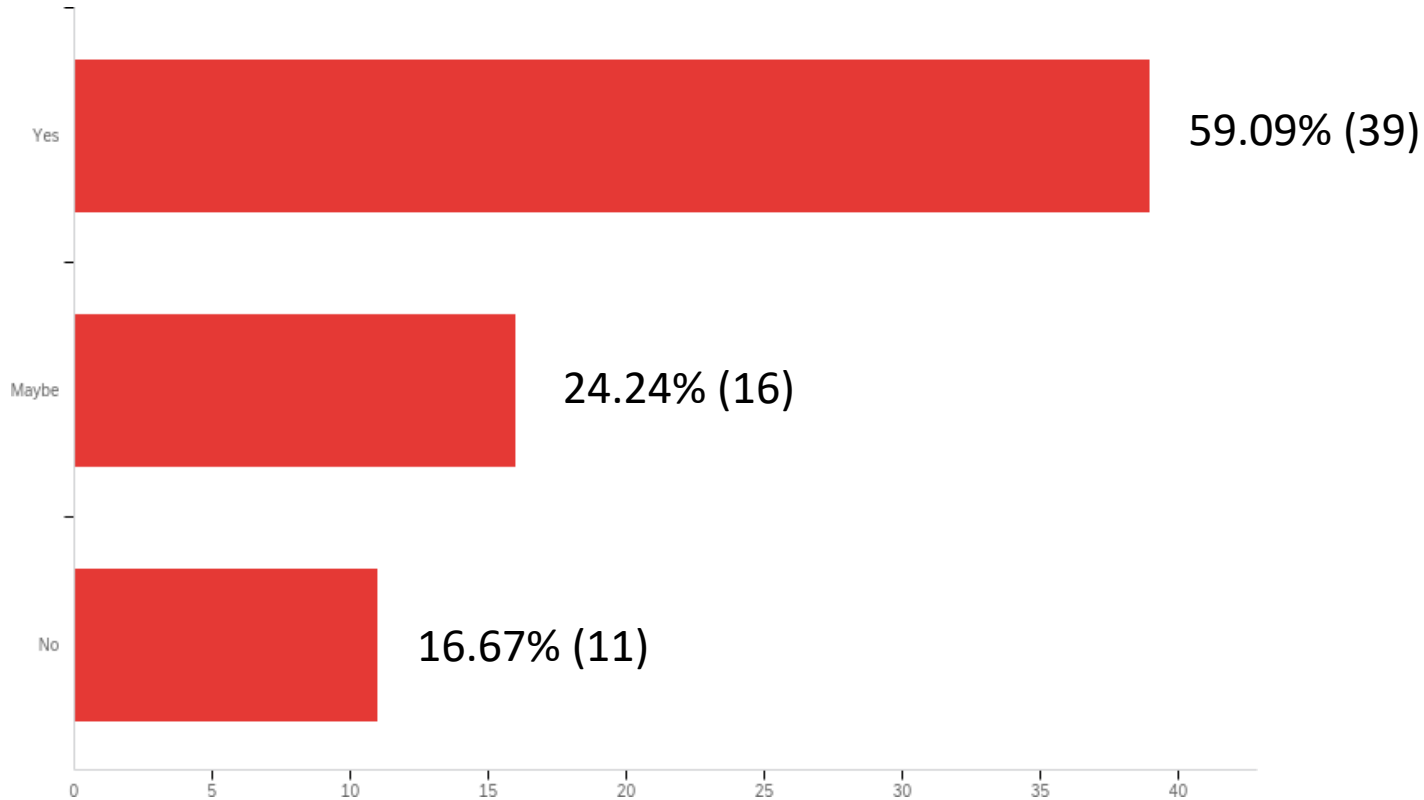
| Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---------|---------|------|---------------|----------|-------|
| 1.00 | 2.00 | 1.71 | 0.45 | 0.21 | 66 |

6. Are cyber threats and cyber crimes a potential issue in your organization? N=66



| Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---------|---------|------|---------------|----------|-------|
| 1.00 | 3.00 | 1.27 | 0.51 | 0.26 | 66 |

7. If you are a current UOG student or if you are intending to enroll as a UOG student in the future, would you be interested in pursuing the Cybersecurity Management Minor as part of your degree program? N=66



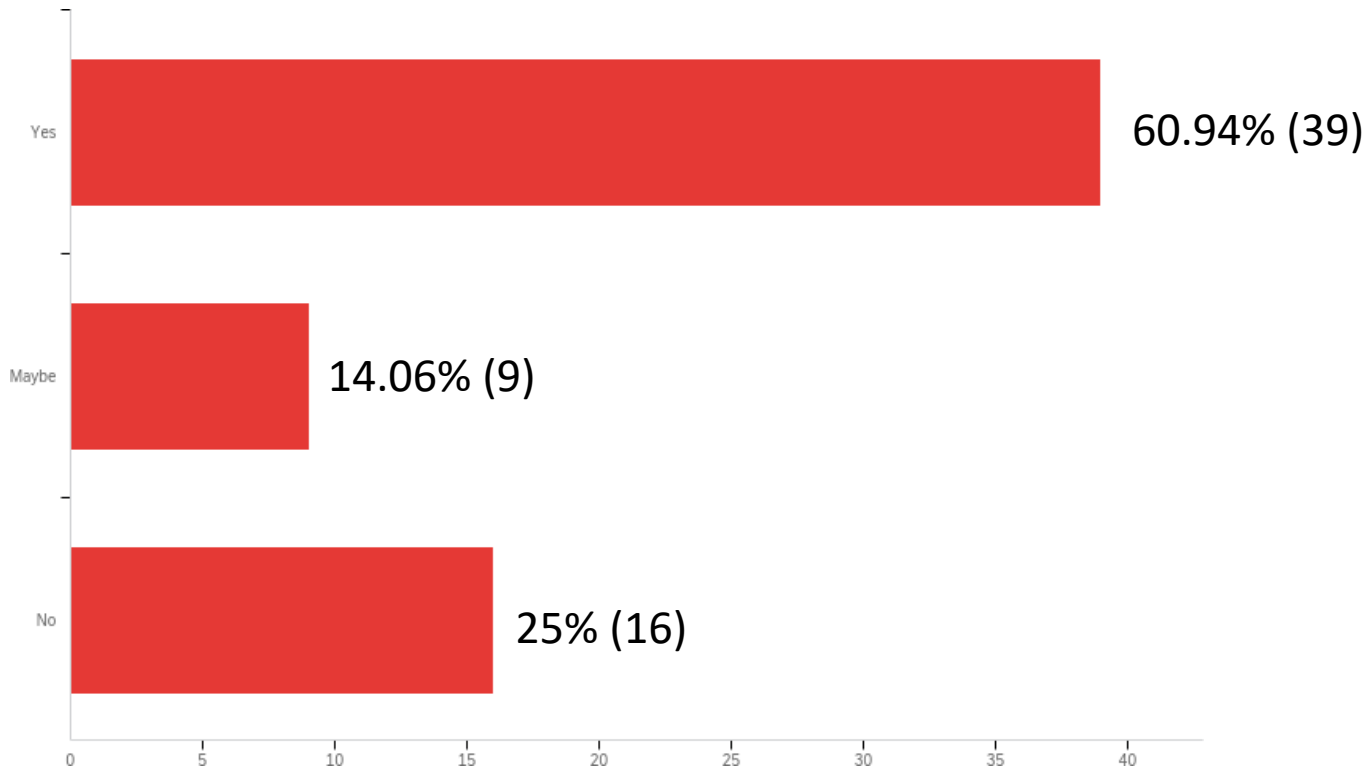
| Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---------|---------|------|---------------|----------|-------|
| 1.00 | 3.00 | 1.58 | 0.76 | 0.58 | 66 |

8. What is your current or intended degree and major at UOG: N=66

| Degree | | |
|--|---|----------------------------|
| N/A (5) | I've already finished an MPA at UOG, but I'd enroll for a distance course | Need to Figure that out :) |
| BS Criminal Justice (4) | | |
| Civil Engineering | Public Administration (4) | |
| Master of Public Administration (9) | | |
| Graduate | Graduated already but would like to obtain Professional Certificate | |
| MPA and will pursue on my masters in education | | |
| Graduated with a Criminal Justice and Public Administration degree | Bachelor of Science (2) | |
| | Professional MBA (3) | |
| | Accounting | |
| Graduate/Alumni (2) | Computer Science (4) | |
| Marine Biology | | |

| | |
|---|---|
| | Engineering |
| BBA/Business (3) | Masters |
| Concentration in International Tourism and Hospitality Management | Currently only have some college credits no degree |

9. Would you like to be contacted by SBPA prior to the launching of the Cybersecurity Management Minor and Professional Certificate Program in Cybersecurity Management in order to consider possible enrollment in the program? N=64



| Minimum | Maximum | Mean | Std Deviation | Variance | Count |
|---------|---------|------|---------------|----------|-------|
| 1.00 | 3.00 | 1.64 | 0.85 | 0.73 | 64 |

10. Would you like to be contacted by SBPA prior to the launching of the Cybersecurity Management Minor and Professional Certificate Program in Cybersecurity Management in order to consider possible enrollment in the program?

| Answer | % | Count |
|--------|--------|-------|
| Yes | 60.94% | 39 |
| Maybe | 14.06% | 9 |
| No | 25.00% | 16 |
| Total | 100% | 64 |






Log No. 6402 Minor & Professional Certificate in Cybersecurity Management

Final Audit Report

2020-06-01

| | |
|-----------------|---|
| Created: | 2020-06-01 |
| By: | Orana Elsegini (oranae@triton.uog.edu) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAAbMZMVO-VgGIZmJoZ8I_1_wC30L76nc0j |

"Log No. 6402 Minor & Professional Certificate in Cybersecurity Management" History

-  **Document created by Orana Elsegini (oranae@triton.uog.edu)**
2020-06-01 - 7:35:33 AM GMT- IP address: 168.123.242.32
-  **Document emailed to Anita Borja Enriquez (abe@triton.uog.edu) for signature**
2020-06-01 - 7:43:48 AM GMT
-  **Email viewed by Anita Borja Enriquez (abe@triton.uog.edu)**
2020-06-01 - 10:48:16 AM GMT- IP address: 104.47.45.254
-  **Document e-signed by Anita Borja Enriquez (abe@triton.uog.edu)**
Signature Date: 2020-06-01 - 10:49:34 AM GMT - Time Source: server- IP address: 114.142.232.35
-  **Signed document emailed to Orana Elsegini (oranae@triton.uog.edu) and Anita Borja Enriquez (abe@triton.uog.edu)**
2020-06-01 - 10:49:34 AM GMT

Signature: 
Christine Mababayag (Oct 23, 2020 08:20 GMT+10)

Email: ckamm@triton.uog.edu

BOR Request- Minor & Professional Certificate in Cybersecurity Management

Final Audit Report

2020-10-22

Created: 2020-10-22
By: Orana Elsegini (oranae@triton.uog.edu)
Status: Signed


Transaction ID: CBJCHBCAABAABcZMATMtYk9wmlRmDRAzj_d-apWib8Xd

"BOR Request- Minor & Professional Certificate in Cybersecurity Management" History

Document created by Orana Elsegini (oranae@triton.uog.edu)

 2020-10-22 - 1:59:31 AM GMT- IP address: 168.123.224.52

Document emailed to Christine Mabayag (ckamm@triton.uog.edu) for signature

 2020-10-22 - 2:12:33 AM GMT


Email viewed by Christine Mabayag (ckamm@triton.uog.edu)

 2020-10-22 - 2:35:30 AM GMT- IP address: 182.173.227.96

Document e-signed by Christine Mabayag (ckamm@triton.uog.edu)

 Signature Date: 2020-10-22 - 10:20:47 PM GMT - Time Source: server- IP address: 182.173.227.96

Document emailed to Thomas W. Krise (tkrise@triton.uog.edu) for signature

 2020-10-22 - 10:20:49 PM GMT

Email viewed by Thomas W. Krise (tkrise@triton.uog.edu)

 2020-10-22 - 10:24:09 PM GMT- IP address: 104.47.45.254

Document e-signed by Thomas W. Krise (tkrise@triton.uog.edu)

 Signature Date: 2020-10-22 - 10:25:06 PM GMT - Time Source: server- IP address: 114.142.241.44

Agreement completed.

20-10-22 - 10:25:06 PM GMT