Professional Masters in
Information and Cyber Security
(PMICS)

Academic and Administrative Rules
Detailed Syllabus of Courses

Department of Computer Science and Engineering
University of Dhaka
Dhaka – 1000

Academic and Administrative Rules

Professional Masters in
Information and Cyber Security

Introduction

The IT industry of Bangladesh is growing very rapidly. We need a vast pool of highly skilled manpower in ICT sector to gear up overall progress of Bangladesh. At the wake of the recent catastrophe in banking sector (ATM hacking, proliferation of Central Reserve), the nation was caught off-guard with its lack of domestic expertise in the field of information and cyber security. In today's world, any country and hence her organizations must be prepared to defend themselves against threats in cyberspace. Department of Computer Science and Engineering envisions that it must respond to this national demand by helping the nation with its resources in building the required skilled manpower in information and cyber security. Hence, its Academic Committee has decided to offer the Professional Masters programs in Information and Cyber Security. This program aims to provide sound theoretical background with excellent practical experience on information and cyber security. This document summarizes the rules and regulations of the program in accordance with the universities newly adopted rules for irregular academic program grouped under the following heads:

I. Title of the Program

This program will be known as "Professional Masters in Information and Cyber Security (PMICS)".

II. Admission Session

There will be two sessions in a year namely Jan-June and July -Dec Session. Students will be admitted in these two sessions.

III. Admission Requirements

Students seeking admission into the PMICS program must have an undergraduate degree in the field of Computer Science, Computer Engineering, Electrical and Electronic Engineering, Electrical and Communication Engineering or any IT/ICT related subjects. Third division in any public examination will not be allowed. If applicable mininum CGPA requirement will be 2.5 or equivalent. Candidates having job experience will be given preference.

IV. Seat Capacity

Maximum seat capacity is 40 for the program. The academic committee of the department will decide on the number of students (not exceeding 40) who will be admitted in a particular semester depending on the available resources.

V. Admission Procedure

Students will be admitted on merit through a written entrance examination and pass mark will be 40%. Student having bachelor/master degree from abroad must have to take equivalence certificate from the equivalence committee of the University of Dhaka. Students shall have to be attached to a hall of the university and get the student identity card from the attached hall. Students of irregular academic program cannot the residential student of a hall and will not be allowed for any privilege of hall.

VI. Duration of the Program

Duration of the program is one year and six month (three semesters). Students are required to complete the degree program within 5 academic years (10 semesters).

VII. Academic activities

Student admission, classroom teaching, laboratory experiment, examination and evaluation, tabulation, publication of result and certificate awarding will be as per this rules described in this document and university's central rule will be applicable for any case that this rules and regulation do not cover.

VIII. Examination and Evaluation

Course teachers will be solely responsible for mid-term, class participation and quiz marks. Final examination will be conducted by the examination committee as per university rules. In case of emergencies, a makeup exam will be arranged subject to the approval of the program conduction committee. Course evaluation will follow the following guideline.

1.	Mid Term/Lab Exam (two)	30%
2.	Class participation	5%
3.	Quiz/term paper/Case presentation/Class test	15%
4.	Final Examination	50%

IX. Grading System

For grading the students, the following Uniform Grading System will be followed as explained below:

Numerical Scores	Letter Grade	Grade Point
80% and above	A+	4.00
75%– less than 80%	A	3.75
70% - less than 70%	A-	3.50
65% - less than 70%	B+	3.25
60% - less than 65%	B	3.00
55% - less than 60%	B-	2.75
50% - less than 55%	C+	2.50
50% - less than 55%	C	2.25
45% - less than 50%	D	2.00
less than 40%	F	0.0
	I	Incomplete
	W	Withdrawn

X. Withdrawal

Withdrawal from the program for a definite period of time may be considered if permission is sought from the Program conduction committee keeping his/her earlier semester grades intact. However, a student must complete the degree within 5 years of his admission into the program. Otherwise, he/she will not be eligible to obtain any diploma.

XI. Retaking a Course

Students with a grade of 'F' in any course may retake the course on payment of requisite fees offered in the subsequent available semester. Student has to pay the full tuition fee for the course. A student earning a grade of 'A-' or worse may also retake a course by paying the requisite fees to improve his/her grade in that course. In order to retake a course, a student must apply to the program conduction committee before the commencement of the semester. All retake application must be approved by the program conduction committee. In case of retake students have to participate in classes, laboratories, in-course and final examination and the higher grade will be considered for degree requirement fulfillment.

XII. Degree Requirements

The program will be consisting of 36 credits of which 27 credits will be course work and 9 credits will be project work. Students completing the required 36 credits within 10 semesters of their admission and with a minimum CGPA of 2.50 will be eligible for the degree. A student's admission will be automatically cancelled, if he/she cannot complete the required 36 credits within 10 semesters of his/her admission with a minimum CGPA of 2.50. The University of Dhaka will award degrees on the recommendation of the Academic Committee of the department.

XIII. Class Time

Classes will start at 6:00 PM on weekdays. In weekend lecture may be arranged as suitable.

XIV. Lecture Method

Classes will be mostly onsite but blended system (online and onsite) may be adopted if necessary. Online class will be no more than 10% of the total classes. In extreme situation online classes might be allowed.

XV. Administration

There will be a three members program conduction committee including chairman as a member formed by the academic committee of the department. Tenure of a program conduction committee will be two years after which all members of the committee except the Chairman of the department must be changed. The tenure of chairman will be limited to the duration of chairmanship. The academic committee of the department will form program conduction committee.

Once served in a program conduction committee in any capacity, a faculty member cannot serve as a member or coordinator of the committee for the next two years. The Academic Committee of the department will be responsible for (a) Admission of students (b) Course Allocation (c) Ensuring logistic support and (d) Formation of examination committee. A teacher will not be allowed to take courses in the irregular academic program more than his/her number of courses in the regular program. Examination committee will work as per university general guidelines and be responsible for conduction of examination, provisional publication of results and compilation and submission of results to the controller of examination for publication. The program conduction committee will generally perform the following functions:

a) Overall coordination of the program
b) Preparation of budgets and maintaining proper accounts
c) Making arrangement for the audit of the accounts
d) Taking decisions relating to pre-requisite courses and course re-takes
e) Assignment of duties and responsibilities to each member of the committee
f) Selection of courses to be offered in each semester
g) Checking course outlines and progress of the courses
h) Conduct teacher's evaluation
i) Submission of periodical reports to the Academic Committee of the department
j) Any other tasks assigned by the Academic Committee of the department

XVI. Instructors/ Co-instructors

Both faculty members of reputed public/private universities and experienced field experts from industry may be appointed as instructors but no more than 30% instructors will be from outside of the

university. Any CSE, DU faculty will be eligible to be appointed as instructor/co-instructor. In case of university teachers other than faculty of CSE, he/she must meet At least ONE of the following criteria

a. Have a PhD degree
b. Be a Professor / Associate Professor

The C&D committee of the department might appoint teachers from other departments of Dhaka University or any other reputed public/private university who satisfies the above criteria. The C&D committee might appoint experts from IT industry as instructors/co-instructors. However, he/she must satisfy BOTH of the following criteria

a. Have a Masters / PhD degree
b. Have 10+ years of experience in working in the field relevant to the subject for which he/she is being considered as a potential instructor. In case of co-instructor only five years of experience in working in the relevant field is required.

XVII. Reserved Regulation:

Rules and regulations not mentioned specifically or not clear in this document will follow the rules and regulations of the irregular academic program of the university.

The Detailed Syllabus of the

Professional Masters in Information and Cyber Security (PMICS) Program

Total Credit: 36

Courses

Course Code	Course Title	Credits
CSE 801	**Communication Protocols and Internet Architecture**	**3**
CSE 802	**Information Security and Cryptography**	**3**
CSE 803	**Software Security**	**3**
CSE 804	**Network and Internet Security**	**3**
CSE 805	**Digital Forensic**	**3**
CSE 806	**Privacy and Ethics**	**3**
CSE 807	**Information Security Management**	**3**
CSE 808	**Cybersecurity Law and Policies**	**3**
CSE 809	**Cloud Security**	**3**
CSE 810	**Project on Cybersecurity**	**9**

Detailed Course Syllabus

CSE 801 Communication Protocols and Internet Architecture

Design, analysis, and implementation of networks and protocols: Internet Architecture & Performance Parameters, TCP/IP, TCP Tahoe, TCP Reno, TCP New Reno, TCP CUBIC, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), Internet Protocol Security (IPsec), Internet Control Message Protocol (ICMP), IPv4 and IPv6, Concepts of routing (Bellman-Ford and Dijkstra algorithms), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhance Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP), Software Defined Networking, Virtual Network Function, OpenFlow Protocol and Network Function Virtualization. **Application layer protocols**: Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), HTTP 1.0 to HTTP 3.0, Cookies, Webcaching, Proxy, Content Distribution Network, Bit Torrent, DASH Protocol, multimedia protocols for voice and video. **Design and Analysis of Networks:** LAN architecture and design, internetworking using switches and routers, the design and analysis of both private networks Internet, Zero trust network architecture. Network quality of service, voice and video on the Internet, policy-based networks, and Introduction to wireless networks – IEEE 802.11 wireless LAN, Adhoc and infrustructure mode networks protocols.

Textbook and Reference:

Textbook:
– *J. F. Kurose and K.W. Ross*, **Computer Networking: A Top Down Approach**, 8th Edition, Pearson Publications, 2020.

References:
– *Andrew Tanenbaum & David Wetherall*, **Computer Networks**, Fifth Edition, Pearson, 2010.

CSE 802 Information Security and Cryptography

Information and Network Security Concepts: Cybersecurity, Information Security and Network Security, CIA triad, Security Attacks, Services and mechanism, Various types of threats and Cryptanalysis. Symmetric Encryption: Symmetric Cipher Model, Classical Substitution and Transposition Ciphers, Block Cipher Design Principles and Data Encryption Standard, Strength of DES, Different variants of DES like 2DES, 3DES. Attack of 2DES, AES. Asymmetric Encryption: Principles of Pubic Key Cryptosystems, RSA, Discrete Logarithm, Diffie-Hellman Key Exchange, Man-in-the- middle attack on Diffie-Hellman. Hash Functions: Applications of cryptographic hash functions, Hash function requirements, Secure Hash Algorithm (SHA), Digital Signatures. Key and Identity Management including certificate management: Key exchange and random numbers, key/identity management, Symmetric key distribution using Symmetric and Asymmetric Encryption, Public Key Distribution, X.509 Certificates, PKI Architecture. User Authentication: Password based authentication, Token based authentication, Biometric authentication, Remote user authentication, security issues for user authentication, AI/ML for security systems.

Textbook and Reference:

Textbook:
– *Willam Stallings*, **Cryptography and Network Security Principles and Practice**, 8th Edition.

CSE 803 Software Security

Overview of software security, types of vulnerabilities, Common Vulnerabilities and Exposure (CVE). **Web security**: Basic three tire model of web architecture, various attacks on web, SQL injection attacks, various types of SQL injection attacks, protection against SQL injection attacks, prepared statements, sanitizing, single origin principle, Cross site scripting attacks/protections, cross site request forgery attacks/protection, case study. **Penetration Testing:** Introduction to common tools used for pen-testing. **Malware analysis**: How malware run, insider attack, backdoors, analysis of brain virus and morris worm, rootkits, botnets, code injection attacks, worm propagation, malware counter measures. Reversing Malware: Introduction to IDA-Pro, ollydbg and REMnux, identifying key x86 assembly logic structure using disassembler, common malware characteristics at windows api level (DLL injection, function hooking etc), recognizing packed malware, manual unpacking of malware using OllyDbg, interacting with malicious websites to examine their nature. **Secure software development**: Secure software development lifecycle, threat modeling, Overview of software analysis methods (formal verification, static analysis, dynamic analysis, model checking). **Secure programming techniques:** input sanitization, canonical representation, internationalization, xss prevention, Content security policy, access control, CSRF prevention, clickjacking prevention, least privilege, thread safe, error handling, handling secrets, SSL library usage, and password storage. Static analysis tools (Fortify SCA). Formal methods for Security, **Buffer and Heap overflow attacks and prevention:** OS security: OS architecture overview, gdb tutorial, c stack frame, conversion of c code to assembly, stack push and pop while function calls, buffer overflow, shell injections, shellcode, call instruction tricks for shell code, integer over

flow, safe/unsafe functions, buffer and heap overflow protections: stack canaries, no execution, address space layout randomization (ASLR), return to libc function chaining, return oriented programming, securing AI/ML systems.

Textbook and Reference:

Textbook:
– *Gary McGraw*, **Software Security: Building Security In**, Addison-Wesley Professional Publication, ISBN: 9780321356703, January 2006.

– *Suhel Ahmad Khan, Rajeev Kumar, Raees Ahmad Khan*, **Software Security Concepts & Practices**, 1st Edition, Chapman & Hall Publication, ISBN 9781032356310, February 13, 2023.

CSE 804 Network and Internet Security

Internet architecture, security flaws on the Internet, **Attacks on networks**: DDOS attacks, reflection attacks, amplification attacks, wireless security, WEP cracking, DNS hijacking, routing attacks, case study: NTP DDOS attack, spamhaus DDOS attack. **Network security at different layers of the OSI and TCP/IP models**: firewalls, security protocols (in particular, IPsec, SSL, and Kerberos), Denial of Service (DoS) attacks/ detection/prevention, viruses and worms, DNS, email & Voice Over IP (VoIP) security, wireless infrastructure security. **Network Intrusion Detection and Analysis**: NIDS/NIPS functionality, Modes and types of NIDS, NIDS/NIPS evidence acquisition, snort rules and alerts, Case study. **Formal methods for modeling and analyzing authorization and access control systems**. **Designing Enterprise systems for Access Control, Authentication and Auditing (AAA)**: Designing networks on selected protocols to support business operations while maintaining identified levels of network security. Supporting secondary network connectivity (wireless, VPNs, BYOD devices, partner networks, cross-domain and other connectivity types). Overview of Information and Network Security Technologies. Overview of Critical Infrastructural Components and Attacks (e.g., Smart Grid, medical systems, smart homes and others), Anomaly detection and attack graphs.

Textbook and Reference:

Textbook:
– *Gary McGraw*, **Information Security: Principals and Practice**, 2nd Edition, John Wiley & Sons, Inc Publication, ISBN 978-0-470-62639-9.

– *Occupytheweb*, **Getting Started Becoming a Master Hacker**, V 1.3.

– *Occupytheweb*, **Networks Basics For Hackers**, V 1.0, InfoSec Press 2023.

– *Occupytheweb*, **Linux Basics For Hackers**, V 1.0, 1st Edition, ISBN-10: 1-59327-855-1.

CSE 805 Digital Forensic

Key digital forensics concepts: Computer forensics, network forensics, mobile device forensics, malware forensics, memory forensics, scientific method of digital forensics, digital evidence, circumstantial vs. digital

evidence, Evidence integrity and cryptographic hash functions, a chain of custody, using forensic copies, reporting and testimony, a case study of real-world crime investigation involving digital forensics. **Legal system in Bangladesh:** Legal system in Bangladesh, criminal vs civil justice system, courtroom scenario, Lawyers vs prosecutors, defense attorneys, law enforcement, warrant requirement, e-discovery, Judges and decision-makers, laws related to cyber crimes and digital forensics, accepted digital evidence in Bangladesh legal system, fingerprint analysis, privacy law, and digital forensics. **Hard Disk and File Systems:** Different types of disk drives and their characteristics, Logical structure of the disk, Booting process of Windows, Linux, and Mac, Various file systems of Windows, Linux, and Mac, storage systems, and Encoding standards. **Defeating Anti-Forensics Techniques**: Anti-forensics techniques, Data deletion and recycle bin forensics, File carving techniques, password cracking techniques, Detecting Steganography and hidden data in the file systems, Anti-forensics countermeasures. **Windows Forensics:** Collect volatile and non-volatile information, Perform Windows memory and registry analysis, Examine cache, cookies and web browser history, Windows files and metadata, Text-based logs, and event-based logs. **Linux and Mac forensics:** Volatile and non-volatile data in Linux, File system analysis in Linux, Mac Forensics. **Network Forensics:** Sources of network-based evidence, Evidence Acquisition: Physical interception, traffic acquisition, and active acquisition, Network intrusion detection and analysis, Event log aggregation, correlation, and analysis, Investigate switch, router, firewall and web proxies. **Mobile Forensics:** Architectural layers and boot processes of Android and ios devices, Investigate cellular network data, SIM file systems and its data acquisition method, Phone locks, rooting of Android and jailbreaking of ios devices, Logical and physical acquisition of Android and ios devices; **Investigating web attacks:** Basics of internet information services logs and Apache web server logs, Functionality of intrusion detection systems and web application firewall, Investigate attacks on web applications and servers. **Malware Forensics:** Static and dynamic analysis of malware, Analyze malware behavior on the system and on the network. **Cloud Forensics:** Basics of cloud computing and cloud forensics, Fundamentals of Amazon web services (AWS) and Microsoft Azure Investigate security incident in AWS and Azure **IoT Forensics:** IoT and IoT security problems, Recognize different types of IoT threats, IoT forensics and perform IoT forensics on IoT devices.

Textbook and Reference:

Textbook:

– *Bill Nelson, Amelia Phillips, Chris Steuart,* **Guide to Computer Forensics and Investigations***,* 6th Edition, Cengage Learning, 2018.

Reference:

– *Nipun Jaswal*, **Hands on Network Forensics**, Packt Publishing Ltd, 2019

CSE 806 Privacy and Ethics

Privacy concepts and policies: technological aspects of privacy - privacy concerns raised by new IT such as the Internet, wireless communications, and computer matching; tracking techniques and data mining; privacy

enhancing technologies; economic aspects - economic models of the market for privacy, financial risks caused by privacy violations, the value of customer information; legal aspects - laissez-faire versus regulated approaches, managerial implications - the emerging role of Chief Privacy Officers, compulsory directives, and self-regulative efforts; and policy aspects trade-offs between individual privacy rights and societal needs. **Privacy enhancing mechanisms**: identity, anonymity, and confidentiality; private data analysis and database sanitization; privacy-preserving data mining techniques including k-anonymity, randomization, differential privacy, federated learning. and secure function evaluation; privacy issues in social networks, RFID, and healthcare applications.

Textbook and Reference:

Textbook:

1. Privacy in Context: Technology, Policy, and the Integrity of Social Life, Helen Nissenbaum, 2009

Reference:

1. Programming Differential Privacy, J P Near and Chike Abuah, 2024
2. Cyber security and Privacy Law Handbook, Walter Rochhi, 2022

CSE 807 Information Security Management

Cyber Security Framework: Critical Success Factors of Information & Cyber Security, Information vs Cyber Security, Cyber Security Layers/Model, Cyber Security Framework (cont.): Common Cyber Threats and Attack Vectors, Cybersecurity Frameworks and Best Practices, Anomaly detection and attack graphs, Information Protection: Asset Classification, Inventory of information and other associated assets, Asset and Data Ownership, Data life cycle, Classification of information with the process, Labelling of information, Information transfer, Access control of information, Acceptable use of information and other associated assets, Data Classification and Sensitivity, Data Encryption Techniques and Algorithms, Secure Data Storage and Backup Strategies. Infrastructure Protection: Secure Network Design and Architecture, Network Access Control and Segmentation, Firewalls, Intrusion Detection, and Prevention Systems, Vulnerability and Configuration Analysis: logic-based and model-based approaches. Access Control and Identity Management: Principles of Access Control and Identity Verification, Role-Based Access Control (RBAC), Privileged Access Management (PAM), Multi-Factor Authentication (MFA), Single Sign-On (SSO), Managing Identity and Authentication, Controlling and Monitoring Access. Risk Management Life Cycle: Risk Assessment, Risk, Threats, vulnerabilities, and misconfiguration analysis, Qualitative and Quantitative Risk Assessment, Risk Management, standard, and best practices, standards (e.g., OCTAVE) and best practices. Risk assessment and Management case study, Risk assessment based on the scenario; Governance & Compliance: Security Policies, Standards, and Procedures (SOP), Working Instructions, User Manual, Work-flow diagram, Security Awareness and Training, ISO, PCI DSS, HIPAA, GDPR and other international standards, InfoSec Risk Based Audit Management Lifecycle, Business Continuity & Disaster Recovery Management: Business continuity program, Disaster Recovery Planning, Incident Response Planning and Preparation, Incident

Detection, Analysis, and Containment, Incident Recovery and Post-Incident Reporting, Proactive and Post-Incident Cyber Services, computer emergency response teams, Cyber Drill, DR Drill.

Textbook and Reference:

1. “Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management" by Thomas R. Peltier
2. "Information Security: Principles and Practices" by Mark S. Merkow and Jim Breithaupt
3. “Information Security Management” by Michael D Workman
4. ”Information Security-The Complete Reference” by Mark Rhodes

CSE 808 Cybersecurity Law and Policies

Introduction to Legal Regulatory Regime regarding Cyber Security in Bangladesh: Cyber Security Act 2023, Digital Security Rules 2020, Evidence (Amendment) Act 2022, Information and Communication Technology Act 2006. Introduction to International Legal Regime Regarding Cyber Security: Budapest Convention on Cybercrime, African Union Convention on Cyber Security and Personal Data Protection, General International Law on Cyberspace (Concept of Sovereignty, Due Diligence, Jurisdiction), Law of International Responsibility, Responsibility of International Organizations in respect of Cybercrime, International Law of Cyber armed Conflict (Concept of Proportionality, Neutrality, Occupation in terms of conducting hostilities). Introduction to Intellectual Property Protection laws in Bangladesh: Copyright Act 2023, Bangladesh Patent Act 2023, Bangladesh Industrial Design Act 2023, Trademark Act 2009 (as amended in 2015), Geographical Indication Act 2013. Introduction to International Legal Regime regarding Data Protection focusing on General Data Protection Regulations (GDPR). Cyber Security Offensive and Defensive Policies used globally in tandem and context with rules and regulations domestically.

Textbook and References

Textbook:

- Chesney, Robert, *Cybersecurity Law, Policy, and Institutions* (version 3.1) (August 23, 2021). SSRN: https://ssrn.com/abstract=3547103 or http://dx.doi.org/10.2139/ssrn.3547103

Reference:

- Schmitt MN. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press; 2017
- *Guide to the General Data Protection Regulation (GDPR)*, Information Commissioner’s Office, (https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf)

CSE 809 Cloud Security

Introduction to Cloud Computing: Definition and applications including benefits, challenges, and risks, Enabling Technologies and System Models for Cloud Computing, **Modern virtualization technologies**

coupled with on-demand IT infrastructures have been widely adopted by industry to save capital and operating expenses. But off-premise on-demand infrastructures give rise to new security concerns. **cloud security**: known risks and vulnerabilities and sound architectural design for secure computing. **Management, governance, audit, legal issues, and meeting regulatory compliance for cloud computing**. Deploying critical security mechanisms related to secure isolation, application security, data protection, access control, privacy, key management, provisioning, identity and authorization management, high-availability, management, and compliance in a cloud-enabled environment. **Understand the concepts and guiding principles** for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services; Approaches to designing cloud services that meets essential Cloud infrastructure characteristics – on-demand computing, shared resources, elasticity and measuring usage. **Design security architectures** that assures secure isolation of physical and logical infrastructures including compute, network and storage, comprehensive data protection at all layers, end-to-end identity and access management, monitoring and auditing processes and compliance with industry and regulatory mandates. **Understand the industry security standards**, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.

Textbook and Reference:

Textbook:
1. *Tim Mather, Subra Kumaraswamy, and Shahed Latif*, **Oreilly Cloud Security and Privacy**,
2. *Chris Dotson*, **O-reilly-security-final-ebook**.

CSE 810 Project on Cybersecurity

A study of and an exercise in developing, leading, and implementing effective enterprise- and national-level cybersecurity programs. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries (such as health, banking, finance, and manufacturing) are discussed. Topics include enterprise architecture, risk management, vulnerability assessment, threat analysis, crisis management, security architecture, security models, security policy development and implementation, security compliance, information privacy, identity management, incident response, disaster recovery, and business continuity planning. A project reflecting integration and application of learning of cybersecurity is included.