



COURSE OVERVIEW IT0180 Cyber Security & Digital Forensics

Course Title

Cyber Security & Digital Forensics

Course Date/Venue

February 08-12, 2026/Tamra Meeting Room, Al Bandar Rotana Creek, Dubai, UAE

Course Reference

IT0180



Course Duration/Credits

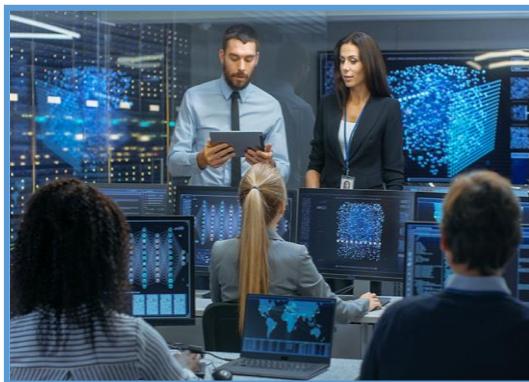
Five days/3.0 CEUs/30 PDHs

Course Description



This practical and highly-interactive course includes real-life case studies where participants will be engaged in a series of interactive small groups and class workshops.

This course is designed to provide participants with a detailed and up-to-date overview of Cyber Security & Digital Forensics. It covers the global cyber threat trends, cyber risks to monetary policy and financial stability; the impact of cyber incidents on public trust, information security principles and frameworks; the cyber security governance and regulatory oversight; and the threat actors, attack vectors, banking systems and critical infrastructure protection.



Further, the course will also discuss the cyber risk assessment and management, malware and advanced persistent threats (APTs); the network security architecture, endpoint and server security; the identity and access management (IAM), data protection, encryption, security monitoring and logging; the cyber incident response framework, cyber incident handling in banking environments and digital forensics; the evidence identification and preservation, disk and file system forensics, memory and volatile data forensics; and the network and log forensics, email, communication forensics, mobile device and cloud forensics.





During this interactive course, participants will learn the financial cybercrime and fraud investigations, insider threat investigations, forensic reporting and expert testimony; the cyber resilience and business continuity, regulatory compliance, audit readiness, cyber security awareness and culture; and the emerging technologies, cyber risks, national and international cyber cooperation and future cyber strategy for central banks.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain an in-depth knowledge on cyber security and digital forensics
- Discuss global cyber threat trends, cyber risks to monetary policy and financial stability and the impact of cyber incidents on public trust
- Explain the information security principles and frameworks including cyber security governance and regulatory oversight
- Recognize threat actors and attack vectors as well as banking systems and critical infrastructure protection
- Carryout cyber risk assessment and management and discuss malware and advanced persistent threats (APTs)
- Describe network security architecture, endpoint and server security
- Carryout identity and access management (IAM), data protection and encryption and security monitoring and logging
- Discuss cyber incident response framework, cyber incident handling in banking environments and digital forensics
- Employ evidence identification and preservation and recognize disk and file system forensics and memory and volatile data forensics
- Identify network and log forensics, email and communication forensics and mobile device and cloud forensics
- Carryout financial cybercrime and fraud investigations, insider threat investigations and forensic reporting and expert testimony
- Apply cyber resilience and business continuity, regulatory compliance and audit readiness and cyber security awareness and culture
- Discuss emerging technologies and cyber risks, national and international cyber cooperation and future cyber strategy for central banks

Exclusive Smart Training Kit - H-STK®



*Participants of this course will receive the exclusive "Haward Smart Training Kit" (H-STK®). The H-STK® consists of a comprehensive set of technical content which includes **electronic version** of the course materials conveniently saved in a **Tablet PC**.*

Who Should Attend

This course provides an overview of all significant aspects and considerations of cyber security and digital forensics for IT and network professionals, cybersecurity and incident response teams, digital forensics and cybercrime investigators, IT managers, risk, and compliance professionals, software developers and cloud engineers and auditors and governance professionals.



Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

Certificate Accreditations

Haward's certificates are accredited by the following international accreditation organizations:

-  [British Accreditation Council \(BAC\)](#)

Haward Technology is accredited by the **British Accreditation Council for Independent Further and Higher Education** as an **International Centre**. Haward's certificates are internationally recognized and accredited by the British Accreditation Council (BAC). BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.
-  [The International Accreditors for Continuing Education and Training \(IACET - USA\)](#)

Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units (CEUs)** in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.



Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:



Dr. George Chel, PhD, MSc, BSc, Prince2, CISCO-CCNA, CISCO-CCENT, is a **Senior Communication & Telecommunications Engineer** with over **20 years** of extensive experience within the **Petrochemical, Oil & Gas** and **Power** industries specializing in **Cybersecurity Methods & Techniques**, **Cybersecurity in Industrial Control Systems (ICS)**, **Cybersecurity Concepts & Principles**, **Secure Network Architecture**, in **Fiber Optics Technology**, **Access Network Planning**, **Fiber Optics Transmission**, **Fiber Optic Cables Construction**, **Optical Drivers & Detectors**, **Fiber Optic Termination**, **Fiber Optic Cables Installation**, **Fiber Optics System Design**, **Media Converters**, **Fiber Optic Systems Testing**, **Optical Fibers Technologies**, **Opto-Electronics**, **Data Networking**, **Access Networks**, **Optical Networks**, DWDM, DSL, FTTH, GPON, **Wireless & Mobile Networks**, **Telecom Technologies**, **Core Network Technologies**, **Broadband Architectures & Services**, **Analogue & Digital Communications**, **IP Networking**, **Network Automation**, **Software Defined Networking (SDN)**, **Network Function Virtualization (NFV)**, **Internet of Things (IoT)**, **Converged Connectivity & Hybrid Access**, **RF Electronics & Digital Communications**, **Communications Systems Analysis**, **Network Security**, **Computer Networks** Modelling & Simulation, **Data Networks & Communications**, **Networking Technology**, **Networking Concepts**, **ICT Systems Management & Strategy**, **Strategic Information Systems**, **Wireless Access Points**, **Analogue & Digital Electronics**, **Circuit Analysis**, **Circuit Design**, **Electromagnetics**, **WiMAX Broadband Wireless System**, **Networking Design & Configurations**, **Practical Industrial Data Communications & Telecommunications**, **Industrial Data Communication Systems**, **Effective Telecoms Strategies**, **Integrated Electro-Optic Devices & Systems**, **Telecom, Datacom & Network**, **EtherNet** Maintenance and Troubleshooting, **Synchronous Digital Hierarchy (SDH)**, **IP Telephony Design (IPTD)** and **LTE Technology (WiMax)** Skills. He is currently the **Core Technologies Section Manager** of Hellenic Telecommunications Organization wherein he is responsible for managing, carrying, conducting, leading and participating in projects relating to the design, evaluation and trial of new aggregation/core network services & systems projects.

During his career, Dr. Chel has gained his practical and field experience through his various significant positions and dedication as the **Deputy Manager**, **Project Manager**, **Lab Section Head**, **Deputy Section Head**, **Program Leader**, **Access Technologies Senior Expert**, **Access Network Development Engineer**, **Telecom Engineer**, **Technical Engineer**, **Senior Expert**, **Senior Technical Instructor/Lecturer**, **Part-Time Lecturer**, **Development Engineer**, **R&D Engineer** and **Research Programmes Engineer**, **Post-Doctoral Research Associate** and **Teaching & Laboratory Assistant** from the Hellenic Telecommunication Organization – Deutsche Telekom Group, Fixed Access Shared Service Center – Deutsche Telekom Technology, OTE Academy, Athens Metropolitan College and Imperial College London.

Dr. Chel has a **PhD in Photonics, Optical Communications & Opto-Electronics** from the **Imperial College London, UK**, a **Master** degree in **Medical Physics & Clinical Engineering** from the **University of Sheffield, UK**, a **Bachelor** degree in **Physics** from the **University of Crete, Greece** and a **Graduate Diploma in Management** from the **University of London, UK**. Further, he is a **Certified Instructor/Trainer**, a **Registered PRINCE2 Project Management Practitioner**, a **Cisco Certified Network Associate Routing and Switching (CCNA)** and a **Cisco Certified Entry Networking Technician (CCENT)**. Moreover, he is an author of many books, technical publication at high-profile scientific journals and conferences and deliver numerous trainings, courses, workshops, seminars and conferences internationally.



Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

- 30% Lectures
- 20% Practical Workshops & Work Presentations
- 30% Hands-on Practical Exercises & Case Studies
- 20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Course Fee

US\$ 5,500 per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the workshop for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1: Sunday, 08th of February 2026

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	PRE-TEST
0830 – 0930	Cyber Security Landscape in the Financial Sector Global Cyber Threat Trends Affecting Central Banks • Cyber Risks to Monetary Policy and Financial Stability • State-Sponsored and Organized Cybercrime Threats • Impact of Cyber Incidents on Public Trust
0930 – 0945	Break
0945 – 1030	Information Security Principles & Frameworks Confidentiality, Integrity, and Availability (CIA Triad) • Defense-in-Depth Security Strategy • Zero Trust Security Model • Risk-Based Security Approach
1030 – 1130	Cyber Security Governance & Regulatory Oversight Role of Central Banks in Cyber Regulation • Cyber Security Policies and Standards • Alignment with International Banking Regulations • Cyber Governance Structure and Accountability
1130 – 1215	Threat Actors & Attack Vectors Cybercriminals, Insiders, and Nation-State Actors • Phishing, Malware, Ransomware, and APTs • Attacks on Payment and Settlement Systems • Insider Threats and Privilege Misuse
1215 – 1230	Break
1230 – 1330	Banking Systems & Critical Infrastructure Protection Core Banking and Real-Time Gross Settlement (RTGS) Systems • SWIFT and Interbank Messaging Security • Digital Payment Platforms and Fintech Risks • Protecting National Financial Infrastructure



1330 – 1420	Cyber Risk Assessment & Management Cyber Risk Identification Techniques • Vulnerability Assessment Concepts • Risk Registers and Treatment Plans • Cyber Risk Reporting to Senior Management
1420 – 1430	Recap Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day One

Day 2: Monday, 09th of February 2026

0730 – 0830	Malware & Advanced Persistent Threats (APTs) Malware Types and Infection Methods • Ransomware Targeting Financial Institutions • APT Lifecycle and Indicators of Compromise • Banking Trojans and Spyware
0830 - 0930	Network Security Architecture Secure Network Design Principles • Firewalls, IDS, and IPS • Network Segmentation and Monitoring • Securing Interbank and External Connections
0930 – 0945	Break
0945 – 1100	Endpoint & Server Security Endpoint Detection and Response (EDR) • Secure Configuration and Hardening • Patch and Vulnerability Management • Privileged Access Control
1100 – 1215	Identity & Access Management (IAM) Authentication and Authorization Models • Multi-Factor Authentication (MFA) • Role-Based and Least-Privilege Access • Managing Privileged Users
1215 – 1230	Break
1230 – 1330	Data Protection & Encryption Data Classification and Handling • Encryption at Rest and in Transit • Key Management Practices • Protecting Sensitive Financial Data
1330 – 1420	Security Monitoring & Logging Security Information and Event Management (SIEM) • Log Collection and Correlation • Detecting Suspicious Activities • Early Warning and Alerting Mechanisms
1420 – 1430	Recap Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day Two

Day 3: Tuesday, 10th of February 2026

0730 – 0830	Cyber Incident Response Framework Incident Response Lifecycle • Roles and Responsibilities During Incidents • Incident Severity Classification • Coordination with National Authorities
0830 – 0930	Cyber Incident Handling in Banking Environments Responding to Payment System Attacks • Managing Ransomware Incidents • Fraud-Related Cyber Incidents • Communication and Escalation Protocols
0930 – 0945	Break
0945 – 1100	Basics of Digital Forensics Purpose and Scope of Digital Forensics • Forensics versus Incident Response • Legal and Regulatory Considerations • Forensic Readiness Concepts



1100 – 1215	Evidence Identification & Preservation Types of Digital Evidence • Chain of Custody Requirements • Evidence Handling Best Practices • Avoiding Evidence Contamination
1215 – 1230	Break
1230 – 1330	Disk & File System Forensics Hard Drive and Storage Analysis • File System Structures • Deleted File Recovery Techniques • Artifact Identification
1330 – 1420	Memory & Volatile Data Forensics Importance of Volatile Data • Memory Acquisition Techniques • Analyzing Running Processes • Detecting Malware in Memory
1420 – 1430	Recap Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day Three

Day 4: Wednesday, 11th of February 2026

0730 – 0830	Network & Log Forensics Network Traffic Analysis • Log Correlation for Investigations • Detecting Lateral Movement • Tracing Attacker Activities
0830 – 0930	Email & Communication Forensics Phishing Investigation Techniques • Email Header and Metadata Analysis • Tracing Spoofed Communications • Evidence Extraction from Messaging Systems
0930 – 0945	Break
0945 – 1100	Mobile Device & Cloud Forensics Mobile Device Evidence Types • Forensics Challenges in Cloud Environments • Data Acquisition Limitations • Legal and Jurisdictional Considerations
1100 – 1215	Financial Cybercrime & Fraud Investigations Digital Fraud Schemes in Banking • ATM, Card, and Payment Fraud Analysis • Cryptocurrency and Digital Asset Investigations • Supporting Financial Crime Cases
1215 – 1230	Break
1230 – 1330	Insider Threat Investigations Indicators of Insider Compromise • Monitoring Privileged User Activity • Digital Evidence in Insider Cases • Coordination with HR and Legal Teams
1330 – 1420	Forensic Reporting & Expert Testimony Structuring Forensic Investigation Reports • Presenting Technical Findings Clearly • Supporting Legal and Regulatory Actions • Maintaining Objectivity and Accuracy
1420 – 1430	Recap Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day Four



Day 5: Thursday, 12th of February 2026

0730 – 0830	Cyber Resilience & Business Continuity Cyber Resilience Concepts • Integration with Business Continuity Planning • Disaster Recovery for Financial Systems • Ensuring Continuity of Critical Services
0830 – 0930	Regulatory Compliance & Audit Readiness Cyber Security Regulatory Expectations • Audit Preparation and Evidence Management • Compliance Monitoring and Reporting • Managing Regulatory Findings
0930 – 0945	Break
0945 – 1100	Cyber Security Awareness & Culture Building a Cyber-Aware Workforce • Social Engineering Awareness Programs • Executive and Board-Level Awareness • Measuring Awareness Effectiveness
1100 – 1215	Emerging Technologies & Cyber Risks Cloud Computing Risks and Controls • Artificial Intelligence and Cyber Security • Blockchain and Digital Currency Risks • Fintech and Open Banking Challenges
1215 – 1230	Break
1230 – 1300	National & International Cyber Cooperation Information Sharing Mechanisms • Coordination with Law Enforcement • Cross-Border Cyber Investigations • Role of Central Banks in National Cyber Defense
1300 – 1345	Future Cyber Strategy for Central Banks Developing a Long-Term Cyber Security Roadmap • Strengthening Digital Forensics Capabilities • Investment in Skills and Technologies • Continuous Improvement and Maturity Assessment
1345 – 1400	Course Conclusion Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course
1400 – 1415	POST-TEST
1415 – 1430	Presentation of Course Certificates
1430	Lunch & End of Course





Practical Sessions

This practical and highly-interactive course includes real-life case studies and exercises:-



Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org



INTERNATIONAL RECOGNITION

