SEVERN BUSINESS COLLEGE

Qualifi Level 5 Diploma in Cyber Security

Course Handbook

Qualification
Qualifi Level 5 Diploma in Cyber Security

Ofqual Number
603/4139/7

Level
5

Total Qualification Time
1200

Credit Value
120

Aim of the Course
This Level 5 Diploma provides the opportunity for individuals to develop a more advanced career in a specific area of business or public organisations by developing analytical knowledge and deeper understandings of several core cyber security operational domains. The course will also provide core information security technical and generic management and leadership teaching. Much of this teaching will be directly relevant to learners moving forward into Information Security Management technical qualifications at the higher-end of the industry market, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP). Qualifi Level 5 Diploma in Cyber Security Specification March 2021 8 At key points, in each unit, learners will be asked to use their own equipment to practise using, and conduct live exercises on, technical IT hardware and software platforms and apps, including Virtual Machines, Linux OS, as well as working beyond the GUI (Graphical User Interface) and into their own Command Lines

Assessment
Assessment is through practical assignments, with no exams - to more accurately reflect the real working environment.

Course Structure

Qualifi Level 5 Diploma in Cyber Security			
Unit number	**Units**	**Unit level**	**Unit credit**
DSC01	Cryptography	5	30
DSC02	Digital Investigations and Forensics	5	30
DSC03	Communications and Incident Management	5	30
DSC04	Strategic Leadership	5	30

Assessment Grades

Marks Ranges %	**Assessment Criteria**
Fail (0-39)	Insufficient information about each assessment criteria
Pass (40-59)	Describe main ideas with evidence on each assessment criteria
Merit (60-69)	Evaluation of ideas with evidence on each assessment criteria
Distinction (70-100)	Critical evaluation of ideas with evidence on each assessment criteria
No Marks	Plagiarism

UNIT SPECIFICATIONS

Unit Title
Cryptography

Level
5

Learning Time Hours
300

Credit Value
30

Unit aim

The process of encrypting and decrypting information forms the basis of much computer, device and network security. Cryptography is designed and used to protect the confidentiality, integrity and authenticity of information. From the very beginnings of computing, and throughout the industry's evolution, the establishment of policies, guidelines and laws has shaped the disciplines of information security and organisational resilience in profound and, often, unintended, ways. In this unit learners will be introduced to the concept and history of cryptography, and its subdisciplines (including cryptology), and how cyber-enabled networks and devices have their communications security underpinned by cryptographic methods and sector standards. Learners will explore methods of attack, including side-channel, additional encryption methods and escrow principles and key. Learners will look at how businesses can deploy encryption to enhance their information security approaches. Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand key cryptographic principles and modes	1.1 Define the concept and application of cryptography 1.2 Explain symmetric and asymmetric modes and approaches 1.3 Assess how cryptographic methods and standards underpin the communications security of cyber-enabled networks and devices
2. Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption	2.1 Explain the key principles of the related standards, regulations and laws and why they are in place 2.2 Assess the consequences for organisations and individuals of non-compliance with these standards, regulations and laws
3. Design an encryption plan and courses of action for a given organisation	3.1 Explain the methods of attack used to target encrypted data 3.2 Assess the additional encryption methods available 3.3 Explain the key principles of escrow and recovery 3.4 Explain the importance of having robust encryption arrangements within IT systems 3.5 Evaluate the existing encryption arrangements 3.6 Design an encryption plan to meet the needs of a given organisation, with recommended courses of actions

Supplementary Text and Reading:

- Gordon Corera (2015) Intercept: The Secret History of Computers and Spies (London: W&N), available at: https://www.amazon.co.uk/Intercept-Secret-History-ComputersSpies/dp/0297871730
- Krebs on Security (Online) accessed at: https://krebsonsecurity.com/
- Lawrence Miller and Peter Gregory (2018) CISSP For Dummies (USA: John Wiley & Sons), available at: https://www.amazon.co.uk/CISSP-Dummies-Computers-Lawrence-Miller/dp/0470537914

UNIT SPECIFICATIONS

Unit Title

Digital Investigations and Forensics

Level

5

Learning Time Hours

300

Credit Value

30

Unit aim

This unit describes and explains how to conduct investigations with cyber-enabled equipment, including on public-internet-facing networks, or other network environments. Much evidence is lost or ruled inadmissible within courts and tribunal environments because it has been mishandled and corrupted (or could have been) by investigators, or those with a perceived chain of custody over the data. Moreover, in a planet of several billion cyber-enabled devices, but few qualified cyber investigators, it is now the case that many organisations have to manage part or all of a cyber incident investigation, because the national CERT or

police/security agencies are otherwise prioritised. In this unit learners will examine the requirements for digital investigations including team formations and tools, understanding the prospects of recovering information, gathering evidential data (including from mobile and IoT devices), safeguarding evidential integrity, as well as the complexity and challenges of storing and presenting evidence within legal environments. Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand the core principles of digital investigations	1.1 Explain the investigation lifecycle from initiation to conclusion 1.2 Explain how a 'digital' domain investigation is organised and managed
2. Apply the types of tool that support professional digital investigations at a strategic level	2.1 Analyse the range of tools that assist digital investigations in different situations 2.2 Select the appropriate tools to carry out a digital investigation for a given situation, justifying the selection
3. Plan for an investigations and forensics teams	3.1 Explain the types of skills required to undertake a variety of investigations and forensic-related work 3.2 Explain dynamics of forming and integrating digital investigation teams and geographically distributed and dispersed investigations and teams 3.3 Develop a plan for the formation of an investigation and forensics teams
4. Understand the importance of safeguarding evidential integrity in digital investigations	4.1 Explain how evidence can be retrieved from mobile devices and IoT devices 4.2 Analyse how evidential integrity is safeguarded during digital investigations 4.3 Assess how evidence is stored and presented within legal environments

Supplementary Text and Reading:

- Bilton, N. (2017) American Kingpin: The Epic Hunt for The Criminal Mastermind Behind the Silk Road (Portfolio)
- Sachowski, j. (2018) Digital Forensics and Investigations: People, Processes and Technologies (CRC Press)
- Sikorski, M and Honig, A., (2012) Practical Malware Analysis (No Starch Press)

UNIT SPECIFICATIONS

Unit Title

Communications and Incident Management

Level

5

Learning Time Hours

300

Credit Value

30

Unit aim

The professional and lawful response to managing an incident can be the difference between company survival or otherwise. Poor responses to major incidents, including mega data breaches, have significantly damaged organisational reputations and financial performance. Significantly mismanaging a cyber incident can result in catastrophic personal and organisational consequences. Such business 'impacts' are covered in-depth within our Threat and Risk units at Levels 2, 3 and 4. and will be explored during this Level 5 unit as part of the contextual case-study learning, and isomorphic reflections, that are central to this unit. In this unit learners will explore the types of site, personnel and equipment required in relation to planning for Incident Management and forming an organisational CERT team (Computer Emergency Response Team). They will then explore the core sub-disciplines and side-disciplines of Cyber Incident Management: Disaster Recovery, Business Continuity Management and Crisis Management. Learners will discuss the importance of the business organisational requirement for skilled and planned communications to operate in combination with advanced and developed management responses and strategy. Learners will develop an understanding of the security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand the physical and human resources required to manage a major suspected cyber security incident	1.1 Explain site-set-up, staffing and organisational arrangements for major suspected cyber-related incidents
2. Apply Business Continuity Management to major incident planning and response	2.1 Assess how Business Continuity Management can be aligned and integrated into a suspected cyber-enabled incident 2.2 Explain the people, assets and processes required within a Business Continuity Plan
3. Understand how Disaster Recovery and Crisis Management are integrated into a suspected major cyber-enabled incident	3.1 Assess how DR and CM strategies and tactics in relation to a suspected major cyber-enabled incident 3.2 Explain the components of good practice in DR and CM plans
4. Evaluate the potential impact of NOT planning crisis communications and incident response	4.1 Evaluate the isomorphic lessons from major cyber breaches and company shutdowns 4.2 Analyse communications approaches and perceived failures in cases of catastrophic business loss related to IT systems failure or attack 4.3 Justify recommendations that would support a cyberresilient approach

Supplementary Text and Reading:

- Austin, L and Jin, Y (2017) Social Media and Crisis Communication (Routledge)
- Richard Bingley (2015) The Security Consultant's Handbook (Ely: IT Governance Press), available at: https://www.itgovernance.co.uk/shop/product/the-security-consultants-handbook
- Heng, G.M (2017) A Manager's Guide to Business Continuity Incidents for Cyber Security Incidents, The Business Continuity Management Institute, available at: https://www.bcm-institute.org/product/a-managers-guide-to-business-continuity-managementfor-cybersecurity-incident-response/

UNIT SPECIFICATIONS

Unit Title

Strategic Leadership

Level

5

Learning Time Hours

300

Credit Value

30

Unit aim

In order for an organisation to be more cyber secure, leadership across employee and stakeholder networks is required to be delivered by the C-Suite. However, what happens if the C-Suite either doesn't listen or doesn't understand the Tier One threat posed by information security vulnerabilities. In this unit learners will develop an understanding of the key features of tech leadership and performance management. Learners will evaluate strategic leadership and management approaches, within a tech sector setting, and what it means to be a 'senior level influencer'. Learners will also develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP). The unit is also highly applicable to learners who are considering taking an MBA, or MBA in Cyber Security, at a later date or who looking to advance into senior management roles within their organisation or sector.

Learning outcomes and assessment criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

Learning Outcome	Assessment Criteria
1. Understand the role senior leaders	1.1 Explain the key roles and responsibilities of senior leaders in a tech sector

and strategic leadership	setting 1.2 Assess how strategic leadership and core goal-setting can enable stronger security cultures
2. Evaluate the management streams and performance monitoring mechanisms that relate to information security	2.1. Explain the importance of integrating management and operational programmes in relation to optimum levels of performance and cyber resilience 2.2 Anlayse the performance monitoring mechanisms in place to protect information security 2.3 Assess how cultural and diversity-related complexities impact on management and performance monitoring
3. Understand how threat and risk identification and management is integrated into C-Suite considerations and governance	3.1 Evaluate risk management and threat identification within the context of wider corporate strategy, responsibilities and governance 3.2 Explain the impact of poor or ineffective C-Suite understanding and direction 3.3 Assess the importance of business ethics and leadership in business values, including within end-user environments of ICT systems
4. Understand how data protection legislation impacts considerations of strategy-setting and strategic leadership	4.1 Evaluate how major data protection laws, impact on CSuite strategic level decision making and strategy setting 4.2 Assess the consequences for individuals and organisations of non-compliance with this legislation

Supplementary Text and Reading:

- Henderson, G. (1994) Cultural Diversity in the Workplace, Praeger
- 'Krebs on Security' cyber security and news blog accessed at: https://krebsonsecurity.com/
- Rumelt, R (2017) Good Strategy: Bad Strategy: The difference and why it matters (Profile Books)

Version:2308a