SEVERN BUSINESS COLLEGE

Qualifi Level 4 Diploma in Cyber Security

Course Handbook

Qualification
Qualifi Level 4 Diploma in Cyber Security

Ofqual Number
603/3331/5

Level
4

Total Qualification Time
1200

Credit Value
120

Aim of the Course
This Level 4 programme 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 useful generic management and leadership teaching at key points in order to help learners to build essential support from within the business for their cyber security work including (but not limited to): Project Management, Risk Management and Business Case writing skills.

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

Course Structure

Qualifi Level 4 Diploma in Cyber Security			
Unit number	**Units**	**Unit level**	**Unit credit**
CSEC01	Cyber Security Threat and Risk	4	20
CSEC02	Network Security and Data Communications	4	20
CSEC03	Database Security and Computer Programming	4	20
CSEC04	Incident Response, Investigations and Forensics	4	20
CSEC05	Security Strategy: Laws, Policies and Implementation	4	20
CSEC06	Cyber Security Threats and Risks: Banking and Finance	4	20

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
Cyber Security Threat and Risk

Level
4

Learning Time Hours
200

Credit Value
20

Unit aim
Cyber security breaches cause significant personal and organisational damage and pose a clear and present risk to business profitability and resilience. Forbes, the business magazine, estimates that the annual cost of cyber-crime might reach (or surpass)

$2Trillion by 2019. At a ground-level, Cyber security breaches are causing business insolvencies and posing challenges to employee safety and wellbeing. In this unit the learner will be introduced to a variety of threats and risks emanating from the cyberspace. The unit will look at various methods of attack and will use case studies to analyse various threat vectors, including Malware, Botnets and Trojans. The unit will introduce and explain various models of measuring threats, risks and impacts. Including, those proposed and recommended by a range of information security standards published by the International Standards Organisation and US NIST (National Institute of Standards and Technology). Using a well-documented 'real-world case study', the learner will investigate and examine the business impact of a recent mega data breach.

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 complex business cyber security threats and risks	1.1 Analyse major cyber breaches and methods of attack that have severely impacted businesses and public organisations 1.2 Examine how to calculate the business impact of a suspected or actual cyber security breach
2. Understand recent mega breaches and explain malware and ransomware attacks	2.1 Apply threat and risk management concepts and models 2.2 Explain the terms malware, ransomware and other forms of intentional malicious cyber attacks
3. Understand how threats and malicious hackers are advancing and developing customised intrusion tools	3.1 Discuss the development of customised intrusion tools and their use by malicious hackers 3.2 Analyse how an intrusion occurred to cause a mega data breach

Supplementary Text and Reading:

- Bingley, R. (2015) The Security Consultant's Handbook, Ely: IT Governance Press
- Krebs on Security (Online) accessed at: https://krebsonsecurity.com/
- Palo Alto Networks (2016) Cyber Security for Dummies (2nd. Ed.) (New Jersey: John Wiley & Sons 2016)

UNIT SPECIFICATIONS

Unit Title

Network Security and Data Communications

Level

4

Learning Time Hours

200

Credit Value

20

Unit aim

In this unit the learner will look at the component parts of digital communications and interoperability with IT networks, hardware, firmware and software components. The inherent insecurity of the internet will be described and discussed. What are the basics of computer science and technology? How do computers communicate with one another? How can networks communicate and how can we plan their security architecture in a more proactive and organised manner? The second half of this unit will look at security planning and core concepts including 'security engineering', systems hardening and cyber resilience.

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 how computers and digital devices communicate with one another over a network	1.1 Analyse the core vulnerabilities within a network environment and an online environment 1.2 Explain how the emergence of security thinking and tools can benefit a network environment
2. Understand, at a strategic level, how computer networking, web applications and software can be exploited	2.1 Evaluate the link between network architecture and security engineering concepts

3. Understand methods of security prevention and systems hardening	3.1 Evaluate internal risks and exposure 3.2 Evaluate available process and physical defences against malicious network intrusions
4. Understand key network security and systems resilience tools, terminology and models	4.1 Explain how key security concepts can be applied in a large and distributed organisation 4.2 Assess how key factors are applied to enhance and embed an holistic approach to network and systems resilience

Supplementary Text and Reading:

- Schneier on Security and the 'CryptoGram' newsletter accessed at: https://www.schneier.com/
- Sikorski, M and Honig, A., (2012) Practical Malware Analysis (No Starch Press)
- Solomon, M. G. Kim, D and Carrell, J. L. Fundamentals of Communications and Networking (Jones & Bartlett, 2014)

UNIT SPECIFICATIONS

Unit Title
Database Security and Computer Programming

Level
4

Learning Time Hours
200

Credit Value
20

Unit aim
Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. Database security is a specialist topic within the broader realms of computer security, information security and risk management. In this unit the learner will explore security risks to database systems and mitigation techniques. Understanding the function of computer programming is essential to understanding the dark arts of 'Black Hat Hackers'. Learners will examine (as a rolling case study) Python as a popular contemporary programming language. The symbiotic link between developments in computer programming and vulnerabilities to hacking will be examined and explored.

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 broad range of information security controls to protect databases	1.1 Explain security risks in database systems 1.2 Assess the effectiveness of information security concepts and tools in protecting databases
2. Understand types of database categories of control	2.1 Explain database terminology and categories of control
3. Understand the underpinning concepts and models of cloud-based storage solutions	3.1 Explore the functionality of database tools available to Data Owners, Custodians, Incident Responders and Investigators
4. Understand the relationship between computer programming and computer hacking	4.1 Explain various popular computer programming languages 4.2 Analyse the relationship between programming skills and the ability to hack into systems
5. Understand the 'interpreted' general-purpose programming language, Python	5.1 Investigate where non-malicious and malicious hackers have utilised Python

Supplementary Text and Reading:

- Alfred Basta & Melissa Zgola (2011) Database Security, Boston: USA: Cengage Learning
- Oracle Database Security Guide, accessed at: https://docs.oracle.com/cd/E11882_01/network.112/e36292/toc.htm
- Mark Lutz (2013) Learning Python (5th Ed.) Newton: USA, O'Reilly Media

UNIT SPECIFICATIONS

Unit Title
Incident Response, Investigations and Forensics

Level
4

Learning Time Hours
200

Credit Value
20

Unit aim
In this unit the learner will examine Incident Response, Computer Emergency Response Teams (CERTS), and events requiring investigative techniques. Learners will identify and examine aligned business tasks and task forces including Disaster Recovery, Business Continuity Management and Crisis Management.
The unit then focuses on exploring cyber-related incident investigations, including evidential analysis gathering, logging and reporting. Learners will have the opportunity to look at case studies and assess how the approaches used could be applied into their own workplace.

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 and composite parts of Incident Response as a business function and how CERTS operate	1.1 Explain the people, structures, processes and tools involved in Computer Incident Responses 1.2 Discuss the different roles within a Computer Emergency Response Team and their importance
2. Understand aligned task/task forces for Business Continuity, Disaster Recovery and Crisis Management	2.1. Explain the terms BC, DR and CM 2.2 Analyse the standards, protocols and concepts underpinning BC, DR and CR and their application within organisations
3. Understand how major computer incidents are formally investigated	3.1 Explain the processes, people and tools used in a planned and structured major incident investigation 3.2 Analyse how evidence is contained, analysed, processed and deployed in a major cyber-related investigation
4. Understand laws and guidance in relation to the conduct of planned and structured major incident investigations	4.1 Examine how relevant laws and professional practice are applied to computer incident investigations

Supplementary Text and Reading:
- Kawakami, J., (2016) Backups: Avoiding computer disasters on Windows, Mac and Linux, John Kawakami Publishing
- 'Krebs on Security' cyber security and news blog accessed at: https://krebsonsecurity.com/
- Luttgens T., Pepe., M. and Mandia, K., (2014) Incident Response & Computer Forensics (3rd Ed.), McGraw Hill Education

UNIT SPECIFICATIONS

Unit Title
Security Strategy: Laws, Policies and Implementation

Level
4

Learning Time Hours
200

Credit Value
20

Unit aim

Knowing how to build a cyber defence strategy, what legal tools require consideration, how policies can be written and embedded, are all vital ingredients to successful in-house cyber security practices. In this unit the learner will bring together knowledge acquired from previous units and build on this in relation to developing plausible strategic plans, executive buy-in and legal compliance. Key questions and challenges are posed:

• What is 'strategy' and what can a 'cyber security strategy' look like?
• How do we achieve senior-level buy-in?
• How do we monitor and safeguard compliance, particularly if our operations are dispersed across a multinational environment?
• What are the key legal requirements and industry standards that can assist and enhance our cyber security strategies and practices?

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 concept of strategy, strategic management, planning and buy-in in relation to cyber security	1.1 Assess the value of strategic management and planning as applied to information security and cyber-enabled business environments
2. Understand how legislation, formal industry standards, training and accreditations support cyber security	2.1 Evaluate key legislation and industry standards that impact and assist cyber security planning 2.2 Assess the key training and accreditation schemes relating to cyber security
3. Understand how to implement Plan, Do, Check and Act security and risk management policies.	3.1 Assess how to design, monitor, implement and continuously improve policies in relation to cyber and information risk business environments.
4. Understand the future legal and technical environment and the impact on cyber security planning and digital risk management	4.1 Investigate the approaches of large influential countries in the information security domain 4.2 Discuss relevant national/international regulatory and standards relating to cyber security environments
5. Understand how to plan and design a security audit for a cyber network	5.1 Design security plans that reflect the legal and political environment

Supplementary Text and Reading:

- ISO (2013) ISO27001:2013 Information Security Management, International Standards Organisation (ISO)
- NIST (Version 1, 2014) or (Version 1.1, 2018) : Cyber Security Framework (NIST CSF): Overview available at: https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
- Touhill, G, and Touhill, T.J (2014) Cyber Security for Executives, New York: Wiley

UNIT SPECIFICATIONS

Unit Title

Cyber Security Threats and Risks: Banking and Finance

Level

4

Learning Time Hours

200

Credit Value

20

Unit aim

In this unit the learner will look at banking and financial services in relation to cyber security threats and risks and the potential methods to mitigate and lessen organisational vulnerability to cyber security attacks. The unit is relevant to anybody who wishes to learn how to identify and plan for direct cyber-attacks on financial services architecture, including those directly employed by the sector, or learners who need to understand their own organisational financial dependencies underpinning financial systems, including payment systems. As 'traditional' financial institutions, financial market platforms, and emerging cryptocurrency markets attract attacks from state and non-state cyber criminals, how can employees and companies protect their own financial infrastructure and supply chains? Case studies, including the TINBA and ZEUS trojans, will be evaluated and discussed.

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 threats and risks facing traditional and emerging financial services	1.1 Analyse how threats and risks to traditional banking and finance platforms and emerging financial impact internal business resilience
2. Understand the architectural structures of traditional and emerging financial markets	2.1 Explain how the financial supply chains for fast-growth medium to large organisations work in financial services 2.2 Discuss how architectural structure relates to cyber security planning considerations
3. Understand how payments systems connect to underpinning financial services architecture	3.1 Assess vulnerabilities and good industry practices related to the payment card Industry 3.2 Apply the PCI DSS standard to your local domain/organisation
4. Understand how crypto currencies connect to underpinning financial services architecture	4.1 Evaluate emerging trends and threats from cryptocurrency-related attacks by cyber criminals

Supplementary Text and Reading:

- British Bankers Association (2014) The Cyber Threat To Banking: A Global Industry Challenge, accessed at: https://www.bba.org.uk/wpcontent/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf
- Cyber Security news reports feed which relate to Cryptocurrency markets: https://www.cybersecurity-review.com/tag/cryptocurrency/
- Kaspersky Research Labs (2015) CARBANAK APT: THE GREAT BANK ROBBERY, accessed at: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

Version:2308a