



# QUALIFI

SUCCESS THROUGH LEARNING  
RECOGNISED WORLDWIDE

## Qualifi Level 2 Diploma Business Beginners in Cyber Security (Last reviewed -April 2019)

## Qualifi Level 3 Diploma in Cyber Security Management and Operations

(Last reviewed -November 2018)

## Qualifi Level 4 Diploma in Cyber Security (Last reviewed -November 2018)

### Specification (For Centres)

*All course materials, including lecture notes and other additional materials related to your course and provided to you, whether electronically or in hard copy, as part of your study, are the property of (or licensed to) QUALIFI Ltd and MUST not be distributed, sold, published, made available to others or copied other than for your personal study use unless you have gained written permission to do so from QUALIFI Ltd. This applies to the materials in their entirety and to any part of the materials.*

## About QUALIFI

QUALIFI provides academic and vocational qualifications that are globally recognised. QUALIFI's commitment to the creation and awarding of respected qualifications has a rigorous focus on high standards and consistency, beginning with recognition as an Awarding Organisation (AO) in the UK. QUALIFI is approved and regulated by Ofqual (in full). Our Ofqual reference number is RN5160.

Ofqual is responsible for maintaining standards and confidence in a wide range of vocational qualifications. QUALIFI is also recognised by Qualifications in Wales (QiW) and the Council for the Curriculum, Examinations and Assessment (CCEA) who are responsible for Awarding Organisations and quality assurance in both Wales and Northern Ireland. QUALIFI is also a signatory to BIS international commitments of quality.

As an Ofqual recognised Awarding Organisation, QUALIFI has a duty of care to implement quality assurance processes. This is to ensure that centres approved for the delivery and assessment of QUALIFI's qualifications and awards meet the required standards. This also safeguards the outcome of assessments and meets national regulatory requirements.

QUALIFI's qualifications are developed to be accessible to all learners in that they are available to anyone who is capable of attaining the required standard. QUALIFI promotes equality and diversity across aspects of the qualification process and centres are required to implement the same standards of equal opportunities and ensure learners are free from any barriers that may restrict access and progression.

QUALIFI's policy document for learners with specific requirements or who need special consideration is available for centre reference. Centres are responsible for reviewing the applicant's ability to complete the training programme successfully and ultimately achieve a qualification. The initial assessment by the centre, will need to take into account the support that is readily available or can be made available to meet individual needs as appropriate. The centre must also consider prior learning and qualifications and they must be in a position to make a judgement on the learner's entry requirements.

## Supporting Diversity

QUALIFI and its partners recognise and value individual difference and have a public duty to promote equality and remove discrimination in relation to race, gender, disability, religion or belief, sexual orientation and age.

## Learner Voice

Learners can play an important part in improving the quality of this course through the feedback they give. In addition to the ongoing discussion with the course team throughout the year, there are a range of mechanisms for learners to feed back about their experience of teaching and learning. This can include questionnaires and surveys to allow both centres and QUALIFI to understand how we can improve the learner experience.

## Contents

Contents .....	3
1 Introduction.....	5
1.1 Why Choose QUALIFI Qualifications? .....	5
1.2 Employer Support for the Qualification Development .....	6
1.3 Qualification Titles and Codes .....	6
1.4 Awarding Organisation .....	6
2 Programme Purpose.....	6
2.1 Reasons for the Qualifications.....	6
QUALIFI Level 2 Diploma Business Beginners in Cyber Security .....	6
QUALIFI Level 3 Diploma in Cyber Security Management and Operations.....	7
QUALIFI Level 4 Diploma in Cyber Security .....	8
2.2 Aims of the Diplomas.....	9
QUALIFI Level 2 Diploma Business Beginners in Cyber Security .....	9
QUALIFI Level 3 Diploma in Cyber Security Management and Operations.....	10
QUALIFI Level 4 Diploma in Cyber Security .....	10
2.3 Learning Outcomes of the Diplomas .....	11
QUALIFI Level 2 Diploma Business Beginners in Cyber Security .....	11
QUALIFI Level 3 Diploma in Cyber Security Management and Operations.....	11
QUALIFI Level 4 Diploma in Cyber Security .....	12
3. Delivering the Qualifications .....	12
3.1 Quality Assurance Arrangements.....	12
3.2 Access to Study.....	13
3.3 Entry Criteria.....	13
4 Structure of the Qualifications .....	14
4.1 Units, Credits and Total Qualification Time (TQT).....	14
4.2 Qualification Structures.....	15
Level 2 Business Beginners in Cyber Security Diploma.....	15
Level 3 Diploma in Cyber Security Management and Operations.....	16
Level 4 Diploma in Cyber Security .....	17
4.3 Progression and Links to other QUALIFI Programmes.....	17
4.4 Recognition of Prior Learning .....	18
5 Guidance to Teaching and Learning .....	18
6 Learner Support.....	19
6.1 Data Protection.....	19
7. Assessment.....	19
8. Course Regulations.....	20
8.1 Course Requirements .....	20
8.2 Classification of Awards.....	20
8.3. Learner Voice.....	21
8.4 Complaints.....	21
9 Equality and Diversity .....	21
10. Further Professional Development and Training .....	23
Appendix 1: Unit Descriptors.....	24
QUALIFI Level 2 Diploma Business Beginners in Cyber Security .....	24
Unit CSB01: Cyber Security: What is 'Hacking'? .....	24

Unit CSB02: Cyber Attack Methods .....	27
Unit CSB03: Computer and Data Use: Law and Regulations .....	30
Unit CSBM04: Mobile Devices and Data: Security Issues and Risks .....	33
Unit CSB05: Cyber Security Network Solutions .....	36
Level 3 Diploma in Cyber Security Management and Operations.....	39
Unit CSM01: Threat and Risk: Expecting the Unexpected.....	39
Unit CSM02: Network Architecture, Communications and Protocols.....	42
Unit CSM03: Mobile Device and Data Risks.....	45
Unit CSM04: Investigations and Incident Response .....	48
Unit CSM05: Solutions: Future-Proofing your Business .....	51
Unit CSM06: EU GDPR and Data Security .....	54
Level 4 Diploma in Cyber Security .....	57
Unit CSEC01: Cyber Security Threat and Risk .....	57
Unit CSEC02: Network Security and Data Communications.....	60
Unit CSEC03: Database Security and Computer Programming .....	63
Unit CSEC04: Incident Response, Investigations and Forensics .....	66
Unit CSEC05: Security Strategy: Laws, Policies and Implementation .....	69
Unit CSEC06: ELECTIVE: Cyber Security Threats and Risks: Banking and Finance .....	72
Unit CSEC07: ELECTIVE: Cyber Wars.....	75

# 1 Introduction

## 1.1 Why Choose QUALIFI Qualifications?

QUALIFI qualifications look to provide a realistic and broad opportunity for learners seeking career and professional development. They will support learners in realising their potential and provide clear objectives.

These objectives are to:

- provide career path support to learners who wish to develop their management skills, enterprise capabilities and opportunities in their chosen sector
- improve learner understanding of any given business environments and organisations and how they are managed and developed
- develop skills and abilities in learners to support their professional development.

Our qualifications provide a rich mix of disciplines and skills development opportunities. Learners will gain insight into the functioning, objectives and processes of organisations, appreciating their diversity and the influences and impact of external forces on them. The fast-changing and complex business environment and different organisational ability to stay resilient and respond positively to change and opportunities will be explored.

Our qualifications will develop learner ability to:

- apply analytical and evaluative techniques and to enhance those skills
- investigate issues and opportunities
- develop their awareness and appreciation of managerial, organisational and environmental issues
- use management techniques and practices in imaginative ways
- make use of relevant information from different sources
- develop and encourage problem solving and creativity to tackle problems and challenges
- exercise judgement and take responsibility for decisions and actions
- develop the ability to recognise and reflect on personal learning and improve their personal, social and other transferable skills.

## **1.2 Employer Support for the Qualification Development**

The development of these qualifications has been initiated and guided by discussions and idea sharing with a range of employers, providers and existing centres demonstrating the rigor, validity and demand for the qualification.

Discussions and feedback have been taken throughout the development of the qualifications on content, the potential learner audience for the qualification and assessment methods, ensuring a valuable experience and a recognised set of skills, knowledge and understanding is realised.

## **1.3 Qualification Titles and Codes**

These qualifications have been accredited to the Regulated Qualification Framework (RQF) and have their own unique Qualification Accreditation Numbers (QAN). This number will appear on the learner's final certification document. Each unit with the qualifications has its own RQF code. The QANs for these qualifications are as follows:

**QUALIFI Level 2 Diploma Business Beginners in Cyber Security (603/3329/7)**

**QUALIFI Level 3 Diploma in Cyber Security Management and Operations (603/3334/0)**

**QUALIFI Level 4 Diploma in Cyber Security (603/3331/5)**

## **1.4 Awarding Organisation**

QUALIFI LTD

## **2 Programme Purpose**

### **2.1 Reasons for the Qualifications**

#### **QUALIFI Level 2 Diploma Business Beginners in Cyber Security**

The qualification has been created to develop those learners who are looking to choose, or already have chosen, a career in a business-related sector but require basic knowledge and competences in the field of Cyber Security (which includes sub-disciplines of compliance, digital media risk management, security risk management, to name a few) without undertaking any technical level of proficiency .

The qualification will:

- prepare learners for employment; and
- support a range of roles that require professional computer use and data management in the workplace.

This basic course is most suitable for executives and managers who are required to use business computers, mobile devices and Wi-Fi-enabled technology in a safe and secure manner that helps to protect their equipment, their business, their colleagues and themselves. They will have some responsibility for business sustainability, profitability, safety and security.

This course is also suitable for any supervisor or manager who has oversight of employees or computer systems infrastructure, but who does not necessarily need to acquire technical proficiency.

Often employees are responsible for colleagues' and customer data located across several time-zones and diverse business environments. This qualification will also incorporate national international legal requirements, critical for those leading and managing the protection of business people, assets and infrastructure. The qualification will identify and evaluate practical ways to safely and securely protect people and information from cyber-attacks and associated impacts.

For more advanced semi-technical and technical Cyber Security Diplomas, please see our Level 3 and 4 Diplomas.

The Diploma is accredited at Level 2 with a total equivalence of 50 credits. It is envisaged that learners completing this Level 2 programme will progress to the QUALIFI Level 3 Diplomas, including our Level 3 Diploma in Cyber Security Management and Operations.

### **QUALIFI Level 3 Diploma in Cyber Security Management and Operations**

The qualification has been created to develop those learners who are looking to choose, or already have chosen, a career in a business-related sector.

It is envisaged that this programme will encourage both academic and professional development so that your learners move forward to realise not just their own potential but also that of organisations across a broad range of sectors.

The rationale of the programme is to provide a career path for learners who wish to develop their core capabilities within the cyber security sector. The outcome of the Diploma, which is a recognised UK qualification, is for learners to develop the skills required by organisations globally.

The qualification will:

- prepare learners for employment; and
- support a range of cyber security-related roles in the workplace.

This qualification is especially designed for organisational executives and leaders who are tasked with responsibility for cyber security, digital risk management, or the oversight thereof. The qualification's primary focus is to prepare administrators and executives to manage and operate generic, non-technical cyber security activities within a business, third sector or government organisation. This course is particularly suited for learners already in full-time work or those seeking to evolve their careers into cyber and information security fields.

The qualification will identify and evaluate practical and lawful ways to safely and securely protect networks, information and assets from cyber-attacks and associated impacts.

This Level 3 qualification is about 'cyber security' as a holistic discipline. It examines both 'cyber' and 'security' domains which relate to IT security. It is therefore in most parts a non-technical qualification that looks at both *cyber-technical* and *cyber-physical* security threats, risks, responses and risk treatments.

The Diploma is accredited at Level 3 with a total equivalence of 60 credits. It is envisaged that learners completing this Level 3 programme will progress to QUALIFI Level 4 Diplomas including the Qualifi Level 4 Diploma in Cyber Security.

#### **QUALIFI Level 4 Diploma in Cyber Security.**

The qualification has been created to develop those learners who are looking to choose, or already have chosen, a career in a business-related sector.

It is envisaged that this programme will encourage both academic and professional development so that your learners move forward to realise not just their own potential but also that of organisations across a broad range of sectors.

The rationale of the programme is to provide a career path for learners who wish to develop their core capabilities within the cyber security and risk management sector. The outcome of the Diploma, which is a recognised UK qualification, is for learners to develop the cyber security skills required by organisations globally. In doing so, the qualification looks to develop the cyber security team leaders, managers and leaders of the future through the creation and delivery of learning appropriate for that industry. It is also to provide a pathway via learner credits and potential direct entry into Level 5 Cyber Security Degree programmes.

The qualification will:

- prepare learners for employment; and
- support a range of senior IT and digital, data and security roles in the workplace.

This Level 4 course is especially designed for existing organisational executives and leaders who are tasked with responsibility for business resilience, information security, technology and risk management, as well as physical safety and security of people, processes and information. Because the course is flexible and online, and utilises many case studies from business and public-sector



organisations, it is particularly suited for those who are already in work, or those who are seeking to develop a structured competency in organisational cyber security and digital data risk management. This course particularly suits learners who work for large multinational firms, international organisations or widely distributed governmental bodies and agencies.

Learners might be employees who are responsible for colleagues' and customer-data located across several time-zones via diverse, international business IT and telecoms networks and environments. This qualification will therefore also incorporate converged security considerations critical for those leading and managing the protection of people, assets and information.

Cyber security considerations have now very much converged with physical security requirements. Due to the course's more advanced technical settings, it is recommended that applicants without any technical experience or understanding of computer networking, network security, programming, or security risk management principles, should complete the QUALIFI Level 3 Diploma in Cyber Security Management and Operations before enrolling onto this course programme.

This Level 4 qualification is potentially unique because it is about 'cyber security' as a holistic discipline. It is therefore a semi-technical qualification that looks at both *cyber-technical* and *cyber-physical* security threats, risks, responses and risk treatments. Due to the huge economic risks to business communities and their underpinning financial infrastructure from cyber-attacks, this course programme provides a dedicated elective unit, *Cyber Security Threats and Risk: Banking and Finance*, in order to thoroughly investigate and analyse how business banking, finance and payment systems are actively targeted, breached and also to ascertain how risks might be treated.

The qualification will identify and evaluate practical ways to safely and securely protect people and information from cyber-attacks and associated impacts.

The Diploma is accredited at Level 4 with a total equivalence of 120 credits. It is envisaged that learners completing this Level 4 programme will progress to QUALIFI Level 5 programmes.

## 2.2 Aims of the Diplomas

### QUALIFI Level 2 Diploma Business Beginners in Cyber Security

The programme provides the opportunity for individuals to forge a career in a specific area of business by seeking a greater knowledge and understanding of cyber and information security, and to support the individual's development into senior positions. The QUALIFI Level 2 Diploma Business Beginners in Cyber Security aims to give learners the opportunity to:

1. develop the knowledge, understanding and skills required for success in employment
2. progress to a related Level 3 professional qualification including the QUALIFI Level 3 Diploma in Cyber Security Management and Operations

3. undertake specialist study relevant to individual vocations and environments in which learners are currently working, or to which learners are aiming to work within the business sector
4. develop their ability to contribute positively to good practice in the business environment through effective use and combination of the knowledge and skills gained in the qualifications
5. develop skills and techniques, personal qualities and attributes essential for safe and secure performance on computer networks and devices in working life and thereby enabling learners to make an immediate contribution to employment.

### **QUALIFI Level 3 Diploma in Cyber Security Management and Operations**

The programme offered provides the opportunity for individuals to forge a career in a specific area of business by seeking a greater knowledge and understanding of cyber and information security, and to support the individual's development into senior positions. The QUALIFI Level 3 Diploma in Cyber Security Management and Operations aims to give learners the opportunity to:

1. develop the knowledge, understanding and skills required for success in employment
2. progress to a related Level 4 professional qualification including the QUALIFI Level 4 Cyber Security Diploma
3. undertake specialist study relevant to individual vocations and environments in which learners are currently working, or to which learners are aiming to work within the business sector
4. develop their ability to contribute positively to cyber security good practice in the business environment through effective use and combination of the knowledge and skills gained in the qualifications
5. develop skills and techniques, personal qualities and attributes essential for successful performance in working life and thereby enabling learners to make an immediate contribution to employment.

### **QUALIFI Level 4 Diploma in Cyber Security**

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. The QUALIFI Level 4 Diploma in Cyber Security aims to give learners the opportunity to:

1. develop the knowledge, understanding and skills required for success in cyber-security-related employment
2. progress into Level 5 learning within Cyber Security domains

3. carry out specialist study relevant to individual vocations and environments in which learners are currently working, or to which learners are aiming to work within business and public service sectors
4. develop their ability to contribute positively to good practice in business technology and risk management environments through effective use and combination of the knowledge and skills gained in the qualification
5. develop skills and techniques, personal qualities and attributes essential for successful performance in working life and thereby enabling learners to make an immediate and positive contribution to their employment.

## **2.3 Learning Outcomes of the Diplomas**

### **QUALIFI Level 2 Diploma Business Beginners in Cyber Security**

Learners studying for the Level 2 Diploma will be expected to develop the following skills during the programme of study:

1. the ability to read and use appropriate literature with a full understanding;  
the ability to think independently and solve problems
2. applying subject knowledge and understanding to address familiar and unfamiliar problems
3. recognising the moral and ethical issues of business practice and research; appreciating the need for ethical standards and professional codes of conduct
4. an appreciation of the interdisciplinary nature of business and service provision
5. capacity to give a clear and accurate account of a subject, in a mature way and engage in debate and dialogue both with specialists and non-specialists
6. transferable skills and knowledge which will enable individuals to meet changing environments and risks.

### **QUALIFI Level 3 Diploma in Cyber Security Management and Operations**

Learners studying for the Level 3 Diploma will be expected to develop the following skills during the programme of study:

1. the ability to read and use appropriate literature with a full understanding;
2. the ability to think independently and solve problems
3. applying subject knowledge and understanding to address familiar and unfamiliar problems
4. recognising the moral and ethical issues of business practice and research; appreciating the need for ethical standards and professional codes of conduct
5. an appreciation of the interdisciplinary nature of business and service provision
6. capacity to give a clear and accurate account of a subject, in a mature way and engage in debate and dialogue both with specialists and non-specialists
7. transferable skills and knowledge which will enable individuals to meet changing environments and risks
8. motivate individuals to progress to further professional development through future study or as part of their chosen career.

## **QUALIFI Level 4 Diploma in Cyber Security**

Learners studying for the Level 4 Diploma will be expected to develop the following skills during the programme of study:

1. the ability to read and utilise relevant technical and security literature (including threat intelligence feeds) with a full understanding; the ability to think independently and solve potential overarching cyber security issues within a business or organisation
2. applying subject knowledge and understanding to address familiar and unfamiliar problems in the cyber security and digital risk management domains
3. recognising the moral and ethical issues of business practice and research; appreciating the need for ethical standards and professional codes of conduct, including in relation to conducting investigations, audits and incident responses
4. an appreciation of the interdisciplinary nature of cyber security within business and service provision and wider operating environments and supply chains
5. capacity to give a clear and accurate account of a subject, in a mature way; engage in credible debate and dialogue both with specialists and non-specialists in relation to cyber security-related issues and challenges
6. transferable skills and knowledge – including Project Management and Incident Response - which will enable individuals to meet changing environments and risks
7. motivate individuals to progress to further professional development through future study or as part of their chosen career
8. instill and embed a sense of understanding and respect of the global nature of the cyber threat environment; as well as the criticality of respecting, anticipating and learning from diverse, international business practices and the global operating context.

These are the overall learning outcomes in line with the Level 2, 3 and 4 Diplomas. The learning outcomes for each unit are identified in Appendix 1 within the unit descriptors.

## **3. Delivering the Qualifications**

### **3.1 Quality Assurance Arrangements**

All centres go through an approval process to be recognised as an approved centre. Centres must have in place qualified and experienced tutors. The experience of tutors and their ability to support learners will be important. Centres must commit to working with QUALIFI and its team of Quality Reviewers/External Verifiers. Continuing professional development (CPD) for tutors is also required.

Approved centres will be monitored by QUALIFI External Quality Reviewers (EQAs) to ensure that learners are provided with appropriate learning opportunities and guidance. EQAs will ask to see and discuss a centre's formative assessment plans. The suitability of these plans will be agreed with the centre.

QUALIFI's guidance on invigilation, preventing plagiarism and collusion will apply to centres. QUALIFI Quality Reviewers/External Verifiers will monitor centre compliance. For assessment purposes, unless otherwise agreed, QUALIFI:

- appoints assignment setters, markers and moderators
- sets and agrees assignments
- marks and moderates assignments
- agrees the final mark and issues certificates.

QUALIFI's 'Handbook on Guidance and Requirements for Assessment and Marking' will apply to its assignment setters, markers and moderators.

### **3.2 Access to Study**

All learners should be invited to an induction event to be introduced to the programme in detail through presentations and discussions with tutors and the centre support team.

All learners should be issued with the Diploma handbook, a timetable and meet with their personal tutor and fellow learners. Centres should assess learners carefully to ensure that they take the right qualification and the right pathways or optional units, to allow them to progress to the next stage.

Centres should check the qualification structures and unit combinations carefully when advising learners. Centres will need to ensure that learners have access to a full range of information, advice and guidance in order to support them in making the necessary qualification and unit choices. When learners are recruited, centres need to give them accurate information on the title and focus of the qualification for which they are studying.

All learners must be registered with QUALIFI within 30 days of centre registration.

### **3.3 Entry Criteria**

The qualifications have been designed to be accessible without artificial barriers that restrict access and progression. Entry to the qualifications will be through centre interview and applicants will be expected to hold the following.

#### **QUALIFI Level 2 Diploma Business Beginners in Cyber Security:**

- qualifications at Level 1 and/or;
- work experience in a business environment and demonstrate ambition with clear career goals;
- a Level 2 qualification in another discipline and who want to develop their careers in business management and/or risk management.

### **QUALIFI Level 3 Diploma in Cyber Security Management and Operations:**

- qualifications at Level 2 and/or;
- work experience in a business environment and demonstrate ambition with clear career goals;
- a Level 3 qualification in another discipline and who want to develop their careers in business management and/or risk management.

### **QUALIFI Level 4 Diploma in Cyber Security:**

- qualifications at Level 3 and/or;
- some technical and risk management experience in a computing or security business environment and demonstrate ambition with clear career goals;
- a Level 4 qualification in another discipline and who want to develop their careers in cyber security.

In certain circumstances, learners with considerable experience but no formal qualifications may be considered, subject to interview and being able to demonstrate their ability to cope with the demands of the programme.

In the case of applicants whose first language is not English, then IELTS 5 (or equivalent) is required. International Qualifications will be checked for appropriate matriculation to UK Higher Education post-graduate programmes. The applicants are normally required to produce two supporting references, at least one of which should preferably be academic.

## **4 Structure of the Qualifications**

### **4.1 Units, Credits and Total Qualification Time (TQT)**

The QUALIFI Business Beginners in Cyber Security is a Level 2 Qualification made up of 5 units equating to 50 credits. All units are 10 credits in value. Each 10-credit unit approximates to a TQT of 100 hours incorporating 60 hours of GLH.  
50 credits equates to 500 hours of TQT.

The QUALIFI Diploma in Cyber Security Management and Operations is a Level 3 Qualification made up of 6 units equating to 60 credits. All units are 10 credits in value. Each 10-credit unit approximates to a TQT of 100 hours incorporating 60 hours of GLH.  
60 credits equates to 600 hours of TQT.

The QUALIFI Diploma in Cyber Security is a Level 4 Qualification made up of 6 units equating to 120 credits. All units are 20 credits in value. Each 20-credit unit approximates to a TQT of 200 hours incorporating 120 hours of GLH.  
120 credits equates to 1200 hours of TQT.

The units have been designed from a learning time perspective and are expressed in terms of **Total Qualification Time (TQT)**. TQT is an estimate of the total amount of time that could reasonably be expected to be required for a learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of a qualification. TQT includes undertaking each of the activities of guided learning, directed learning and invigilated assessment.

Examples of activities that can contribute to Total Qualification Time include:

- guided learning
- independent and unsupervised research/learning
- unsupervised compilation of a portfolio of work experience
- unsupervised e-learning
- unsupervised e-assessment
- unsupervised coursework
- watching a prerecorded podcast or webinar
- unsupervised work-based learning.

Guided Learning Hours (GLH) are defined as the time when a tutor is present to give specific guidance towards the learning aim being studied on a programme. This definition includes lectures, tutorials and supervised study in, for example, open learning centres and learning workshops. Guided learning includes any supervised assessment activity; this includes invigilated examination and observed assessment and observed work-based practice.

Some examples of activities that can contribute to guided learning include:

- classroom-based learning supervised by a tutor
- work-based learning supervised by a tutor
- live webinar or telephone tutorial with a tutor in real time
- e-learning supervised by a tutor in real time
- all forms of assessment that take place under the immediate guidance or supervision of a tutor or other appropriate provider of education or training, including where the assessment is competence-based and may be turned into a learning opportunity.

## **4.2 Qualification Structures**

### **Level 2 Business Beginners in Cyber Security Diploma**

There are mandatory units for this qualification. All units cover a number of topics relating to learning outcomes. Each unit has the equivalency of 10 credits.

Learners are required to complete the five mandatory units to achieve the 50 credits required to gain the Level 2 Business Beginners in Cyber Security Diploma. Learners will be expected to attend lectures and workshops that will introduce the subject matter. Formative assessments (weighted at 0%) may be used in lectures or tutorials to check knowledge and understanding of specific topics and subject areas. Units require reflective exam sets and/or summative assessments for marking.

Unit Reference	Mandatory Units	Level	Credit	TQT	GLH
CSB01	Cyber Security: What is 'Hacking'?	2	10	100	60
CSB02	Cyber Attack Methods	2	10	100	60
CSB03	Computer and Data Use : Laws and Regulations	2	10	100	60
CSB04	Mobile Device and Data: Security Issues and Risks	2	10	100	60
CSB05	Cyber Security Solutions	2	10	100	60

### Level 3 Diploma in Cyber Security Management and Operations

There are mandatory units for this qualification. All units cover a number of topics relating to learning outcomes. Each unit has the equivalency of 10 credits.

Learners are required to complete the six mandatory units to achieve the 60 credits required to gain the Level 3 Diploma in Cyber Security Management and Operations. Learners will be expected to attend lectures and workshops that will introduce the subject matter. Formative assessments (weighted at 0%) may be used in lectures or tutorials to check knowledge and understanding of specific topics and subject areas. Units require reflective exam sets and/or summative assessments for marking.

Unit Reference	Mandatory Units	Level	Credit	TQT	GLH
CSM01	Threat and Risk: Expecting the Unexpected	3	10	100	60
CSM02	Network Architecture: Communications and Protocols	3	10	100	60
CSM03	Mobile Device and Data Risks	3	10	100	60
CSM04	Investigations and Incident Response	3	10	100	60
CSM05	Solutions: Future-Proofing your Business	3	10	100	60
CSM06	EU GDPR and Data Security	3	10	100	60



## Level 4 Diploma in Cyber Security.

There are mandatory and optional units for this qualification. All units cover a number of topics relating to learning outcomes. Each unit has the equivalency of 20 credits.

Learners are required to complete six units (five mandatory units and one elective unit) to achieve the 120 credits required to gain the Level 4 Diploma in Cyber Security. Learners will be expected to attend lectures and workshops that will introduce the subject matter. Formative assessments (weighted at 0%) may be used in lectures or tutorials to check knowledge and understanding of specific topics and subject areas. Units require reflective exam sets and/or summative assessments for marking.

Unit Reference	Mandatory Units	Level	Credit	TQT	GLH
CSEC01	Cyber Security Threat and Risk	4	20	200	120
CSEC02	Network Security and Data Communications	4	20	200	120
CSEC03	Database Security and Computer Programming	4	20	200	120
CSEC04	Incident Response, Investigations and Forensics	4	20	200	120
CSEC05	Security Strategy: Laws, Policies and Implementation	4	20	200	120
Unit Reference	Elective Units	Level	Credit	TQT	GLH
CSEC06	Cyber Security Threats and Risk: Banking and Finance	4	20	200	120
CSEC07	Cyber Wars	4	20	200	120

### 4.3 Progression and Links to other QUALIFI Programmes

Learners completing the **QUALIFI Level 2 Diploma in Business Beginners in Cyber Security** can progress to:

- the QUALIFI Level 3 Diploma in Cyber Security Management and Operations, or
- directly into employment in an associated profession.

Learners completing the **QUALIFI Level 3 Diploma in Cyber Security Management and Operations** can progress to:

- the QUALIFI Level 4 Diploma in Cyber Security, or
- directly into employment in an associated profession.

Learners completing the **QUALIFI Level 4 Diploma** can progress to:

- a Higher Education Level 5 course in Cyber Security, or
- directly into employment in an associated profession.

#### **4.4 Recognition of Prior Learning**

Recognition of Prior Learning (RPL) is a method of assessment (leading to the award of credit) that considers whether learners can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess, and so do not need to develop through a course of learning.

QUALIFI encourages centres to recognise learners' previous achievements and experiences whether at work, home or at leisure, as well as in the classroom. RPL provides a route for the recognition of the achievements resulting from continuous learning. RPL enables recognition of achievement from a range of activities using any valid assessment methodology. Provided that the assessment requirements of a given unit or qualification have been met, the use of RPL is acceptable for accrediting a unit, units or a whole qualification.

Evidence of learning must be valid and reliable. For full guidance on RPL please refer to QUALIFI's policy document on RPL.

## **5 Guidance to Teaching and Learning**

To ensure consistency and quality of delivery amongst centres, QUALIFI has outlined a number of policies and procedures required to ensure the very best standards are available to learners. These include:

- expertise of staff
- learning and teaching methods
- study skills
- learning resources
- personal development planning
- career opportunities.

The policies and procedures are available on request to all accredited centres or to those wishing to apply for accreditation to deliver QUALIFI qualifications.

## 6 Learner Support

Centres should continue to support learners and encourage appropriate behaviour. To ensure consistency and quality of delivery amongst centres QUALIFI, has outlined a number of policies and procedures to ensure the very best standards are available to learners. These include:

- learners with disabilities
- health and safety
- conduct
- progression
- weekly timetable/attendance requirements.

The policies and procedures are available on request to all accredited centres or to those wishing to apply for accreditation to deliver QUALIFI qualifications.

### 6.1 Data Protection

All personal information obtained from learners and other sources in connection with studies will be held securely and will be used during the course and after they leave the course for a variety of purposes. These should be all explained during the enrolment process at the commencement of learner studies. If learners or centres would like a more detailed explanation of the partner and QUALIFI policies on the use and disclosure of personal information, please contact QUALIFI via email [support@QUALIFI-international.com](mailto:support@QUALIFI-international.com)

## 7. Assessment

These qualifications are vocational as they can support a learner's career progression. To meet QUALIFI's aim to provide an appropriate assessment method each unit will be assessed through tasks that will be written in a way to make them realistic 'work-related' tasks wherever possible. Learners will need to demonstrate knowledge, understanding and. Original thought, problem solving and recommendations on actions will also be asked for from learners where appropriate for the unit. Intellectual rigour will be expected appropriate to the level of the qualification.

Assignments will contain a question strand for each of the given unit's learning outcomes. The assignment tasks will address the LO (learning outcome) and AC (assessment criteria) requirements. Within assignments there will always be requirements for learners to engage with important and relevant theory that underpins the subject area.

The assignment questions will require learners to draw on real organisations to illustrate their answers. To support this activity during the programme of learning, centres are required to make sure that they include case studies of relevant organisations and, wherever possible, facilitate in-company opportunities for learners to undertake research and investigation projects and/or support the organisation with various tasks. Mature and part-time learners will ideally be able to draw on their personal work experience too.

Sample assessments and marking scheme are available on request as part of the Qualification Specification supplied to centres.

QUALIFI has an assessment policy and procedure documents that are available to all centres delivering this qualification. QUALIFI's 'Handbook on Guidance and Requirements for Assessment and Marking' covers the following:

- assessment strategy
- assessment arrangements for learners with a disability
- verification
- marking scheme/pass mark
- deferral after valid mitigating circumstances
- referral after failure
- dealing with difficulties in meeting assessment deadlines
- late submissions
- assessment boards
- appeals
- cheating and plagiarism
- referencing
- confidential material
- submission.

## **8. Course Regulations**

### **8.1 Course Requirements**

Learners must complete all required units and pass the appropriate mark to receive the full Diploma.

A mark of at least 40% is required for a unit to be passed and the credit achieved. This same pass mark applies to all units that contribute to the Diploma.

QUALIFI will issue certificates to all successful learners through the registered centres.

### **8.2 Classification of Awards**

Where a candidate has achieved an overall average mark of at least 70% from all the units, QUALIFI may award a Distinction, although offering such a grade to individual candidates is at the discretion of QUALIFI, and is not normally given after any successful referral attempts.

Decisions about the overall classification of awards are made by QUALIFI through the application of the academic and relevant course regulations. It is based on the Average Percentage Mark (APM) or, at the discretion of QUALIFI, on the basis of your overall profile and performance subject to the minimum requirements.

### 8.3. Learner Voice

Learners can play an important part in improving the quality of this course through the feedback they give. In addition to the ongoing discussion with the course team throughout the year, there is a range of mechanisms for learners to feed back about their experience of teaching and learning.

### 8.4 Complaints

QUALIFI recognises that there may be occasions when learners and centres have cause for complaint about the service received. When this happens, the complaints procedure is intended to provide an accessible, fair and straightforward system that ensures as an effective, prompt and appropriate response as possible.

For more information on our formal complaints procedure please contact in the first instance or email: [support@QUALIFI-international.com](mailto:support@QUALIFI-international.com)

## 9 Equality and Diversity

QUALIFI recognises that discrimination and victimisation are unacceptable and that it is in the interests of QUALIFI employees to utilise the skills of the total workforce. It is our aim to ensure that no employee or other representative of QUALIFI receives less favourable facilities or treatment (either directly or indirectly) in recruitment or employment on grounds of age, disability, gender/gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex, or sexual orientation (protected characteristics).

Our aim is that our workforce will be truly representative of all sections of society and each employee feels respected and able to give their best. We oppose all forms of unlawful and unfair discrimination or victimisation. To that end the purpose of this policy is to provide equality and fairness for all.

Our staff will not discriminate directly or indirectly, or harass customers or clients because of age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, and sexual orientation in the provision of QUALIFI's goods or services.

This policy and the associated arrangements shall operate in accordance with statutory requirements, particularly the Equality Act 2010 <https://www.gov.uk/equality-act-2010-guidance>. In addition, full account will be taken of any guidance or codes of practice issued by the Equality and Human Rights Commission, any government departments, and any other statutory bodies.

The policy document will be monitored and reviewed annually and can be downloaded from our website or by making contact with QUALIFI.



## 10. Further Professional Development and Training

QUALIFI supports UK and international customers with training related to our qualifications. This support is available through a choice of training options offered through publications or through customised training at your centre.

The support we offer focuses on a range of issues including:

- planning for the delivery of a new programme
- planning for assessment and grading
- developing effective assignments
- building your team and teamwork skills
- developing student-centred learning and teaching approaches
- building in effective and efficient quality assurance systems.

You can request customised training through your registered centre in the first instance. If you need to contact QUALIFI directly:

Our customer service number: +44 (0) 115 882323

Or email: [support@QUALIFI-international.com](mailto:support@QUALIFI-international.com)

Website: [www.QUALIFI.net](http://www.QUALIFI.net) [www.QUALIFI-international.com](http://www.QUALIFI-international.com)

## Appendix 1: Unit Descriptors

### QUALIFI Level 2 Diploma Business Beginners in Cyber Security

#### Unit CSB01: Cyber Security: What is 'Hacking'?

Unit code: Y/617/1124

RQF level: 2

#### Aim

What is 'hacking' and why is it so important? In this unit the learner will explore the history and different approaches to the common term known as 'hacking'. What is hacking? Where does the terminology derive from? Why is it important to the development of technology and the vulnerability of Information Communication Systems?

This unit will then examine the impacts of malicious hacking on businesses, organisations and individual people. Case studies, including video and audio, will be used to describe scenarios whereby malicious hacking has caused severe loss to a business and/or personal distress to individuals. By covering the underlying causes and consequences of hacking, learners will be able to begin to understand the wide range of risk management scenarios that businesses are required to plan for in terms of securing and preparing their organisations against cyber threats.

#### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand computer hacking mindsets and goals and the clear difference between malicious and non-malicious hacking	1.1 Define the term 'computer hacking' 1.2 Describe types of malicious and non-malicious hacking, using recent examples 1.3 Explain the difference between malicious and non-malicious hacking 1.4 Describe why an organisation might be targeted
2 Understand the impacts of hacking on individuals and organisations	2.1 Describe how malicious hacking can impact individuals 2.2 Describe how hacking can severely affect organisations 2.3 Outline basic legal consequences of becoming involved in malicious hacking, and of being impacted by hacking
3.1 Understand different types of hacker and their possible motivations	3.1. Explain why people carry out hacking activities, using recent examples 3.2 Describe the major risks an organisation faces from a malicious cyber-attack



## Indicative Content

- What is 'cyber security' and what does a 'cyber-attack' look like?
- What is 'hacking'?
- Malicious v non-malicious hacking: understanding the boundaries between research and cyber crime
- Case studies on the negative impacts of 'Black Hat' hacking
- Business, financial and reputational Impacts upon the organisation
- Impacts on the person and family
- Impact assessment: identifying and reporting on organisational risk

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources that is provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the learning outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Learner Journal).

## Assessment Guidance

Each unit in the qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the five (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: REPORT: What assets might we lose in a cyber-crime attack on a major business? Describe and explain realistic potential impacts for an imagined company (or one that you work in/with)? (Maximum 500 words.)

## Suggested Resources

Bingley, R. (2015) *The Security Consultant's Handbook*, Ely: IT Governance Press

Hackmageddon website: Cyber Security Threats and Statistics: accessed at: <http://www.hackmageddon.com/>

Krebs on Security (Online) accessed at: <https://krebsonsecurity.com/>

## Unit CSB02: Cyber Attack Methods

Unit code: D/617/1125

RQF level: 2

### Aim

In this unit, the learner will look in more detail at the most common types cyber-attack on business communities. How do they spread? What methods do the hackers use when conducting malicious attacks?

The unit will investigate the difference in becoming a victim of a targeted attack, or of an untargeted breach. What does a cyber attack look like? How can end-users tell if they have been hacked or potentially compromised?

The key to cyber security is being proactive in identifying threats and risks to organisations. The unit ends by providing a sources and structure for what is known as 'Cyber Threat Intelligence', a critically important sub-sector to the cyber security industry.

### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the most common types of cyber-attack methods on business communities	1.1 Describe the most popular types and methods of cyber-attack on business networks and business end-users
2 Understand the difference between targeted and untargeted cyber-attacks	2.1 Explain the impact of targeted and untargeted attacks 2.2 Describe how to assess individual and organisational risks and vulnerabilities
3 Understand how to assess whether a device has been hacked	3.1 Describe the visual symptoms that suggest a device has been hacked 3.2 Describe the processes to follow to confirm if a device has been hacked 3.3 Apply Cyber Threat Intelligence approaches to given organisational threats

## Indicative Content

- Most common cyber threats to business networks
  - Case studies in systems attacks – WannaCry, Equifax, Banking and Finance
  - Targeted v untargeted attacks: why it's good to know who's attacking us
  - How to tell we've probably been hacked
  - Understanding 'Cyber Threat Intelligence' and the provision of key CTI information sources
- Risk assessment: Likelihood versus Impact

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in the qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the five (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: Threat Report: Describe and briefly explain the five most likely cyber-attacks for your workplace. In a matrix table, calculate the Likelihood and Impact (out of a maximum measurement of 5 for five of your threats. (Maximum – 750 words)

## Suggested Resources

CESG and CERT UK (2014), 'Common Cyber Attacks: reducing the Impact', accessed and downloaded on 28/04/2017 at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/400106/Common\\_Cyber\\_Attacks-Reducing\\_The\\_Impact.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf)

CNET (15/05/2017): 'How to protect your businesses from ransomware' (2.18), accessed on 12/06/2017 at: <https://www.cnet.com/how-to/wannacry-ransomware-how-to-protect-your-pc/>

LifeWire.com (09/05/2017), 'Patch Tuesday', accessed on 12/05/2017 at: <https://www.lifewire.com/patch-tuesday-2625783>

## Unit CSB03: Computer and Data Use: Law and Regulations

Unit code: H/617/1126

RQF level: 2

### Aim

In this unit the learner will explore some of the major national and international laws that govern computer and data use. Among other significant pieces of legislation, this unit will focus on the EU General Data Protection Act (GDPR). This regulation (and laws similar to it within national jurisdictions) can lead to severe penalties for companies that experience deliberate or unintentional causes of data breaches, which result in the loss of customer or employee personal data. Basic approaches to data security – including protecting data at rest and data in transit - are covered.

This unit will also cover computer misuse laws. This is important as students will discover that there are many laws to deter computer crime (including theft, vandalism and bullying) that can lead to severe criminal or civil law sanctions: including fines, a criminal record and jail-time.

### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the wide-ranging laws and regulations that computer and data use are subject to	1.1 Outline the main laws and regulations relating to computer and data use
2 Understand the core and components of the EU General Data Protection Regulation and similar legislation	2.1 Describe how EU GDPR, and similar legislation, impact businesses in an international trading environment 2.2 Discuss ways to protect data in transit and data at rest
3 Understand how legal frameworks protect personal and workplace data	3.1 Describe the criteria for Personal Data under EU GDPR and other major jurisdictions (including UK and USA) 3.2 Describe the legal sanctions applied to those who become involved with computer misuse 3.3 Explain the legal requirements to report suspected computer and data crime to the relevant authorities

## Indicative Content

- Computer crime laws: How have they been applied against hackers?
- Computer Misuse, Data Protection and Fraud Acts (UK as a case study)
- EU GDPR and how it impacts global business and multinational organisations
- Preeminent laws and regulations for international business compliance
- Protecting data at rest and data in transit

## Delivery Guidance:

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in the qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the five (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: Research and describe the most important data security laws and regulations that apply to your workplace. Suggest some methods to protect your organisation's data in order for that organisation to remain legally compliant (Maximum - 750 words.) *Learners will need to state the country and sector that they work, or hope to work in.*

## Suggested Resources

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>

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>

Geoffrey Sampson (2017) *Law for Computing Students* (BookBoon or Ventus of Denmark) available at: <https://bookboon.com/en/law-for-computing-students-ebook>



## Unit CSBM04: Mobile Devices and Data: Security Issues and Risks

Unit code: K/617/1127

RQF level: 2

### Aim

The number of smartphone users is forecast to grow to around 2.5 billion in 2019. According to Cisco, the IT corporation, some 50 billion Wi-Fi enabled devices will be connected to the internet by 2020. These days many of us want to live our lives and go about our business 'on the move'. In this unit the learner will examine how mobile devices and other cyber-enabled devices are at severe risk of hacking. This unit will identify and assess the types and value of data held within mobile devices. The unit will cover what is meant by the term the 'Internet of Things' and why IoT devices are vulnerable to hacking. The unit will close by exploring how users can take practical steps to prevent the loss of data on mobile devices including smartphones, iPhones, iPads and tablets.

### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand basic security flaws and issues in relation to mobile devices	1.1 Explain key cyber security lapses and challenges in relation to mobile devices 1.2 Describe key threats posed to mobile devices and Wi-Fi enabled devices from malicious hacking
2 Understand basic security flaws and issues in relation to the Internet of Things	2.1 Explain key cyber security lapses and challenges in relation to the Internet of Things
3 Understand solutions for protecting mobile devices and data	3.1 Describe methods used to protect a range of mobile devices and the related data

## Indicative Content

- How mobile devices work and their communications vulnerabilities
- Main attack types launched against mobile devices
- Calculating the loss of our mobile data
- Main security issues relating to the Internet of Things
- IoT – what’s the right security strategy?
- The security industry approach: 10 recommended solutions for protecting mobile devices and data

## Delivery Guidance:

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the five (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Imagine that you have been put in charge of the Bring-Your-Own-Device security policy in your workplace. What five additional security measures would you recommend that your organisation implements, and why? (Maximum of 750 words).

## Suggested Resources

Action Fraud website (UK police and fraud intelligence bureau website with online cyber-crime alerts): <https://www.actionfraud.police.uk/>

Balaban, D., (12/06/2017): 'Opinion: Beware of the next wave of cyber threats: IoT ransomware', accessed on 14/06/2017 at: <https://www.information-management.co/opinion/beware-of-the-next-wave-of-cyber-threats-iot-ransomware>

CBS News (24/02/2016) Cyber thieves hacking victims through mobile apps, accessed on 14/06/2017 at: <https://www.youtube.com/watch?v=0M8BM64jfAO>

## Unit CSB05: Cyber Security Network Solutions

Unit code: M/617/1128

RQF level: 2

### Aim

In this unit the learner will bring together their prior learning from the other units on the course. The unit will focus on protecting and future-proofing the learner's network environment; the Local Area Networks and Wide Area Networks (including databases and storage) of the business.

The learner will look at security architecture and security engineering as very basic concepts and to understand key security management approaches to protecting information. Information assets can include people, processes and technology. The learner will then build on this to design their own organisational cyber security plan. The goal of the plan will be to ensure that their own organisation's IT infrastructure is much safer than beforehand. Because 'cyber security' is a discipline that converges physical and technical security requirements, much of this unit content will provide the learner with Crime Prevention Through Environmental Design Principles (CPTED) that include a strong element of physical security content as well as an introduction to Business Continuity and Disaster Recovery practices and principles.

### Learning and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the importance of having the correct mindset when using ICT	1.1 Explain the importance of personal attitude and approach, and organisational awareness training, in relation to managing and reducing cyber security risks
2 Understand how physical security adjustments and knowledge of CPTED principles can strengthen cyber security plans	2.1 Describe a range of physical security approaches that protect against malicious and non-malicious cyber security incidents 2.2 Outline the key CPTED principles and their application to cyber security plans
3 Understand the ISO27001 Information Security Management Standard, and other useful Standards and Education programs	3.1 Explain how planning can be informed and shaped by existing standards
4 Develop a computer/network security plan ('toolkit') for a selected organisation	4.1 Describe the key requirements of the security toolkit in relation to the organisation's security needs and priorities 4.2 Design a cyber security toolkit to meet the security requirements of an organisation

## Indicative Content

- Personal attitudes to computer use and how to change organisational cultures
- CPTED, security engineering and physical/environmental security measures
- Protecting critical business processes
- Applying International Standards, Useful Networks and Industry Educational approaches
- Designing a cyber security toolkit for a workplace organisation

## Delivery Guidance:

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the five (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Formative assessment: describing the most important laws and standards that impact cyber security planning .

Summative Assessment: Presentation of cyber security toolkit – for treating a nominated organisation's cyber risks (maximum 15 slides with accompanying 'notes' for assessor to read)

### **Suggested Resources**

Cryptzone (2015), 'Preventing Cyber Attacks with a Layered Network Security Model: Risk mitigation based on the principles of Zero Trust', can be accessed by applying via the organisation's website at: <http://www.cryptzone.com/forms/preventing-cyber-attacks-layered-network-security-whitepaper>

Executive Order 13636 (12/02/2013), 'Improving Critical Infrastructure Cybersecurity', was accessed and downloaded on 26/06/2015 at: <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>

ISO27001 (2013), The Information Security Management Standard. Overviews of all of the ISO standard relating to Information Systems security can be found at: <https://www.iso.org/isoiec-27001-information-security.html>

SANS Critical Security Controls – Version 5: was accessed on 26/06/2015 at: <https://www.sans.org/critical-security-controls/>

## Level 3 Diploma in Cyber Security Management and Operations

### Unit CSM01: Threat and Risk: Expecting the Unexpected

Unit code: T/617/1163

RQF level: 3

#### Aim

In this unit the learner will be look at various case studies in recent cyber-attacks on business organisations, public sector agencies and individual victims. They will then conduct analysis will then into the motivations of malicious hackers. This analysis will include basic geopolitical learning, as it relates to the cyber domain, as well as identifying how and why different industry sectors (including Banking and Finance) are particularly vulnerable.

Towards the end of the unit the learner will look at the types of hacking undertaken: White Hat hacking, Grey Hat hacking and Black Hat Hacking. Learners will be introduced to concepts such as 'Threat', 'Risk', 'Security Engineering', 'Cyber Threat Intelligence' and 'Cyber Resilience'.

#### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand key business cyber security concepts including 'threats' and 'risks'	1.1 Explain major cyber events and methods of attack that have severely impacted businesses 1.2 Explain sources of cyber security threats and risks
2 Understand effective sources of Cyber Threat Intelligence	2.1 Explain cyber intelligence and the most effective sources 2.4 Explain how organisations can proactively plan and calculate the risks and threats to prioritise remediation (risk-assessment) 2.5 For a chosen global region, review how the IT function within a multinational organisation reports on and plans for cyber security threats and risks
3 Understand the 'psychology' of computer misuse and the associated terminology	3.1 Assess the factors that put individuals at risk from a cyber-attack 3.2 Explain the attack-lifecycle 3.2 Describe the potential risks from a deliberate, planned attack, from a malicious hacker or group

## Indicative Content

- Cyber security and current attack trends and terminology
  - Motivation of those who carry out cyber-attacks and the impacts
  - Case studies in attacks and impacts on business organisations
- Geopolitical and sectoral considerations in the domain of cyber threat-management
- The role and sources of Cyber Threat Intelligence
  - Security engineering and asset protection principles in the sphere of Information Security

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*Video-shelf:* Unit content and additional information provided by the course leader via video

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).



## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: CONSULTANCY REPORT: Produce a Regional Risk Report on Cyber threats for your (or another) business organisation. Provide a description of at least five threats to this business and provide an 'Impact' score out of 5 for each of these threats, in a separate attached table. (1=Low impact, 2=Moderate, 3=Medium, 4=High, 5=Catastrophic) (Maximum 1,000 words.)

## Suggested Resources

Bingley, R. (2015) *The Security Consultant's Handbook*, Ely: IT Governance Press

Palo Alto Networks (2016) *Cyber Security for Dummies*, New Jersey: John Wiley & Sons 2016

Krebs on Security, cyber security news feed, accessed at: <https://krebsonsecurity.com/>

## Unit CSM02: Network Architecture, Communications and Protocols

Unit code: F/617/1165

RQF level: 3

### Aim

In this unit the learner will look at IT networks and the various components and architecture as they relate to the topic of 'cyber security'. This unit will break down the processes involved in IT network-based communications and protocols and introduce and explain the OSI Model of computer communication and interoperability. One dedicated lesson will address: 'How does the internet work?' The learner will develop an understanding of the more popular and destructive methods used to carry out attacks including case studies in Botnets, Trojans and other Malware. Key information security principles - including the 'CIA Triad' and 'Access Controls' – are introduced and explained within a business organisational context.

This unit prepares learners to participate in the often-technical aspects of change management and configuration management committees and task groups that might be responsible for aspects of organisational cyber security. A range of industry case studies will be used throughout this unit in order to upskill the learner and provide an 'helicopter' view of network architecture, communications and underpinning protocols.

### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand computer networking environments and ICT operate at a strategic level within a business organisation	1.1 Explain direct risks and threats to different types of network configurations within business organisations 1.2 Describe the OSI Model layers and 1.3 Apply these within your formal risk assessment summative assessment
2 Understand the threats and risks posed to LANs and WANs within a business organisation	2.1 Assess defensive and offensive cyber security strategies and frameworks to protect LANs and WANs from threats and risks 2.2 Explain how the internet works and why it is non-hierarchical 2.3 Explain how computer programming works and why it is a fundamental issue to consider within an information security plan
3 Understand the importance of identifying and prioritising risk treatments	3.1 Calculate cyber threats and risks by way of a formal Risk Assessment for an organisation 3.2 Recommend remediation (treatments) within part of a formal Risk Assessment process for an organisation

## Indicative Content

- Communication and network principles and protocols: the OSI Model
- How the internet works
- Network security devices, Local Area Networks (LAN) and Wide Area Networks (WAN)
- Information Security Frameworks: The CIA Triad and Access Controls
- Computer programming: how it relates to hacking and cyber systems risk exposure
- Conducting formal risk assessments for business organisations
- Prioritising and recommending risk treatments/remediation for business environments

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit accumulating credits as they pass each unit assessment point.

During each of the **six** (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Formative Assignment: design a quantitative risk assessment for your home network.

Summative Assignment: (RISK ASSESSMENT: – Design and explain a risk assessment matrix for cyber security in your chosen business organisation – maximum 1000 words).

## Suggested Resources

NIST (2014) *Framework for Improving Critical National Infrastructure*, see 'Risk Assessment' section, accessed and downloaded on 25/01/2018 at: <https://www.securitymagazine.com/articles/86754-best-practices-for-conducting-a-cyber-risk-assessment>

Schneier on Security and the 'CryptoGram' newsletter accessed at: <https://www.schneier.com/>

Solomon, M. G. Kim, D and Carrell, J. L. *Fundamentals of Communications and Networking* (Jones & Bartlett, 2014)

Whitman, M.E. & Mattord, H.J. (2009) *Principles of Information Security*, Boston: Cengage

## Unit CSM03: Mobile Device and Data Risks

Unit code: J/617/1166

RQF level: 3

### Aim

Mobile devices pose a significant threat to an organisation's state of cyber security. The number of smartphone users is around 2.5 billion at time of writing. On any single day, hundreds of millions of employees travel and commute and are mobile-enabled in terms of conducting their business and exposing valuable data to enhanced risk.

In this unit the learner will learn how mobile devices become attached to radio and telecommunications networks. How are they connected to the internet and what types of tool can be utilised by malicious attackers to harm individuals and business organisations?

The second half of this unit will introduce and explain significant favoured ways by the cyber security and mobile device industry used to protect mobile devices and data. Key approaches and tools such as data encryption, storage back-up, and other security measures will be investigated and recommended.

Moreover, Cisco estimates that 50 billion items will be connected to the internet by 2020. The Internet of Things (IoT) are cyber-enabled gadgets and devices – often used for leisure or household purposes - that unintentionally expose our home or business networks to additional risk because they become attached to the very same communications channels and signals. In response, malicious hackers are developing customised malware to attack such devices. What are the IoT vulnerabilities and how can they be patched or remediated, if at all? Analysis or consideration of the IoT will therefore form an important part of this unit.

A range of case studies for business and public sector/government organisations will be used throughout this unit.

### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand how mobile smartphones and the Internet of Things communicate and the associated risks	1.1 Explain mobile smartphone vulnerabilities and the associated risks 1.2 Explain vulnerabilities of the Internet of Things and the associated risks of these device connections and signals
2 Understand risks posed by malware and mobile apps	2.1 Assess how various types of malware and monitoring (sniffing) devices can connect with mobile device/s
3 Understand commonly recommended mobile device protection methods advocated by the tech industry	3.1 Explain mobile device security solutions that are suitable and tailored to different types of user and business environment 3.2 Recommend Mobile Device Management (MDM) within organisational information security plans, as part of ISO27001 compliance

## Indicative Content

- Vulnerabilities and associated risks
  - How mobile device communications work
  - Protecting mobile data: network security on devices: android (OS), Wi-Fi networks and security management
  - The Internet of Things: vulnerabilities and consideration within wider security planning
  - Malware attacks on mobile devices
  - Case studies of mobile data breaches
  - Counting the cost of data loss from mobile device intrusion
  - Security solutions: generic and bespoke
- Mobile device protection methods

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing ,as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the **six** (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: Devise a formal workplace REPORT on mobile data risks (including IoT considerations) specific to their organisation for a Board of Directors meeting. The REPORT should include a realistic and fully-costed Courses of Action chapter at the end of the document. (Maximum words: 1000.)

## Suggested Resources

Android Authority website: <https://www.androidauthority.com/>

ISO27001 (2013), The Information Security Management Standard. See section 6.2.1 that relates to Mobile Device Management (MDM):

<https://www.iso.org/isoiec-27001-information-security.html>

Joint Information Systems Committee JISC (2012), *Security, Mobile devices and Data Protection*, accessed and downloaded on 21/12/2017 at: <https://www.jisc.ac.uk/guides/security-mobile-devices-and-data-protection>

## Unit CSM04: Investigations and Incident Response

Unit code: R/617/1168

RQF level: 3

### Aim

Investigations and Incident Response are different operations within the discipline of Information Security. However, they are closely related.

In this unit the learner will investigate techniques used to identify and investigate suspicious computer incidents. Learners will learn about the essential roles, responsibilities, tasks and sub-disciplines within Incident Response. The learner will become familiar with the essential functions of Computer Emergency Response Teams (CERTS) and Incident Response (IR), Disaster Recovery Planning and Business Continuity Management (BCM), including documentation and review.

The learner will also explore investigations as a discipline and how the approaches and concepts of investigations (such as Forensics and Seizure) can be applied to an ICT incident. All unit sections will include descriptions and suggestions about relevant SIEM, Incident Response and Investigations tools. Many of these monitoring and recovery tools can be used to conduct workplace investigations in an ethical and professional manner. A range of case studies for business and public sector/government organisations will be used throughout this unit.

### Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the core phases, tools and processes of Incident Response and putting together a CERT	1.1 Explain the terms Incident Response and CERT 1.2 Explain key information, stages and personnel to be included in any professional IR plan 1.3 Describe how CERTs are put together and who is included
2 Understand Disaster Recovery (DR) and Business Continuity Management (BCM) as disciplines to support a cyber incident response team	2.1 Explain the terms Disaster Recovery (DR) and Business Continuity Management (BCM) 2.2 Analyse how BCM and DR considerations are applied to an overall organisational computer IR plan
3 Understand how organisations can investigate major incidents related to suspected cyber security attacks	3.1 Apply the rules and principles of investigation to an Incident Response to ensure that potential evidence is successfully recovered and stored in an uncontaminated manner



## Indicative Content

- Incident Response and CERTS
- Incident Response plans
- Disaster Recovery and Business Continuity Management
- Investigations and digital forensics
- Reporting and recording investigative activity
- Legal and ethical principles of cyber investigations, audits and IR

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the **six** (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Produce an INCIDENT MANAGEMENT PLAN for a business enterprise for a suspected (but not proven) major malicious cyber-attack. (Maximum: 1,000 words.)

## Suggested Resources

Luttgens T., Pepe., M. and Mandia, K., (2014) *Incident Response & Computer Forensics* (3<sup>rd</sup> Ed.) McGraw Hill Education 2014

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>

Toigo J., in TechTarget (2017) *Storage disaster recovery plans must account for weather threats*, accessed and downloaded on 21/11/2017 at: [http://searchdisasterrecovery.techtarget.com/opinion/Storage-disaster-recovery-plans-must-account-for-weather-threats?utm\\_content=eru-rd2-rcpD&utm\\_medium=EM&asrc=EM\\_ERU\\_85757347&utm\\_campaign=20171122\\_ERU%20Transmission%20for%2011/22/2017%20\(UserUniverse:%202475935\)&utm\\_source=ERU&src=5692049](http://searchdisasterrecovery.techtarget.com/opinion/Storage-disaster-recovery-plans-must-account-for-weather-threats?utm_content=eru-rd2-rcpD&utm_medium=EM&asrc=EM_ERU_85757347&utm_campaign=20171122_ERU%20Transmission%20for%2011/22/2017%20(UserUniverse:%202475935)&utm_source=ERU&src=5692049)

## Unit CSM05: Solutions: Future-Proofing your Business

Unit code: R/617/1171

RQF level: 3

### Aim

In this unit the learner will bring together your knowledge and understanding from the previous units. This unit focuses on scoping the threats and vulnerabilities to companies, employees and customers across their entire network space, including LANs, WANs, Cloud Storage, mobile devices and any IoT-enabled devices

The learner will apply the OSI model to understand the various opportunities that business organisations can take to protect their people, processes and technologies. The learner will then begin the task of developing an holistic security plan for a large-scale business organisation.

Learners will explore various Security Engineering Standards and Threat Assessment approaches before devising and generating their own organisational security plan based on a formal risk assessment. This plan should be comprehensive, relevant and suitable to be applied by a multinational organisational Executive Board.

### Learning and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the future cyber threat environment for companies in the short to medium term	1.1 Discuss key emerging cyber-enabled workplace technologies and the associated cyber security risks 1.2 Apply formal information security management approaches to a complex modern workplace environment
2 Understand how formal Industry Standards, Training and Accreditations support cyber security and business resilience	2.1 Explain the key industry standards relating to cyber security and business resilience 2.2 Explain the key training and accreditation schemes relating to cyber security and business resilience
3 Develop a cyber security plan ('cyber security business toolkit') for a large business organisation	3.1 Explain the costings and 'business case' for investing in a lawful internal cyber security system 3.2 Design a cyber security toolkit (security plan) to meet the security requirements of an organisation that is based on a formal risk assessment for the same organisation

## Indicative Content

- Emerging technologies: including Robotics, Augmented Reality and AI, Cloud Sprawl
- Information Security Standards
- Information Security education and networking bodies
- Designing cyber security risk assessments and generating from this a cyber security plan (business toolkit)

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the **six** (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: The learner should produce a cyber security plan that is based upon a formal risk-assessment. Presentation Format (PowerPoint or similar): Maximum 20 slides.

## Suggested Resources

Computer Ethics Institute, *10 Commandments of Computer Ethics*, accessed at: <http://computerethicsinstitute.org/publications/tencommandments.html>

HR Magazine (2016), *HR's Role in Dealing with Terror Threats*, accessed at: <http://hrmagazine.co.uk/article-details/hrs-role-in-dealing-with-terror-threats>

ISO (2013) *ISO27001:2013 Information Security Management*, International Standards Organisation (ISO)

*SANS 20 Critical Security Controls*, can be accessed at: <https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download>

## Unit CSM06: EU GDPR and Data Security

Unit code: Y/617/1172

RQF level: 3

### Aim

The European Union (EU) impacted most global enterprises in May 2016 when it passed the General Data Protection Regulation, entering into effect two years later (May 25, 2018). All companies—including international firms—doing business with individuals located in EU member states must comply with the regulation's far-reaching provisions. Moreover, many significant trading nations, including the UK, are emulating the EU GDPR to pass their own upgraded data protection regulations for citizens. Failure to act quickly to prepare for the regulation could have serious consequences—to an organisation's bottom line, customer relationships and reputation.

In this unit the learner will develop an understanding of EU GDPR legal provisions and how these have been interpreted and implemented at a national level. Learners will have the opportunity to use your understanding to create an in-house EU GDPR audit toolkit.

Where appropriate, a range of case studies for business and public sector/government organisations will be used throughout this unit.

### Learning and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand EU GDPR, and similar legislation	1.1 Explain the core aspects of the EU GDPR and similar legislation 1.2 Assess how this legislation impacts on identifying and collating personal data 'held' by an organisation
2 Understand legal interpretations of and implementation approaches to the EU GDPR at a national level	2.1 Analyse the diversity of approaches and considerations, at a national level, implementation and enforcement of EU GDPR
3 Develop an in-house EU GDPR audit toolkit	3.1 Assess the factors to take into account to ensure organisational compliance and security needs are met 3.2 Based on own assessment, design an in-house EU GDPR audit toolkit to meet the needs of an organisation

## Indicative Content

-What does EU GDPR cover? Underpinning ethos/objectives in relation to protecting personal data

Other relevant legislation

-Reviewing and collating an organisation's overall data properties

-Developing an EU GDPR implementation project plan

-Case studies in data insecurity

-Design your own EU GDPR audit toolkit

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **10 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the **six** (10-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Design an EU GDPR Audit toolkit for your actual or imagined workplace organisation – maximum 1,500 words

## Suggested Resources

Allen & Overy (2017) The EU General Data Protection Regulation, accessed at: <http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>

EU GDPR Official Portal from the European Union can be accessed at: <https://www.eugdpr.org/>

Zorz, M., (2017) An example EU GDPR Toolkit from expert firm HelpNet.com: <https://www.helpnetsecurity.com/2017/11/14/eu-gdpr-documentation-toolkit/>



## Level 4 Diploma in Cyber Security

### Unit CSEC01: Cyber Security Threat and Risk

Unit code: T/617/1129

RQF level: 4

#### 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

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
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

## Indicative Content

- What are 'threat' and 'risk' in a computer security environment?
- Cyber security, current attack trends, methods and terminology
- Case studies in 'mega breaches', malware and ransomware attacks: what can we learn?
- Security and risk assessment: models and how to conduct analysis, including those recommended by ISO and NIST
  
- Cyber Threat Intelligence: Directing, Analysing, Disseminating, Action-On
- Business Impact Analysis

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six 20-credit units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: (Assessment: CONSULTANCY REPORT: Post-incident Business Impact Assessment (BIA) report reviewing a publicly documented mega data breach with personal and organisational impacts. (Maximum 1500 words.)

## Suggested Resources

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* (2<sup>nd</sup>. Ed.) (New Jersey: John Wiley & Sons 2016)

## Unit CSEC02: Network Security and Data Communications

Unit code: K/617/1130

RQF level: 4

### 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

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
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

## Indicative Content

- Network principles and protocols, security and systems resilience tools
- Security Engineering: Access controls, the CIA triad, systems hardening
- Software development and how it relates to cyber security risks
- Web applications and how they relate to risk
- Other key methods of malicious network attack
- Preventing and mitigating network attacks
- Cyber Resilience: Change Management and Configuration Management

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (20-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: MALWARE – Explain how ransomware was used to attack a given case study organisation. What measures could have been put in place to prevent or lessen the attack's impact? (Maximum 2,000 words.)

## Suggested Resources

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 CSEC03: Database Security and Computer Programming

Unit code: M/617/1131

RQF level: 4

### 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

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
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

## Indicative Content

- Database security breach types
- How various types of databases organise data, including the Grandfather-Father-Son model of Disaster Recovery
- Categories of control and the Anderson Rule
- Case studies in big data organisation and breach incidents
- Impact and utility of Cloud-based approaches
- Differences between compiled and interpreted programming languages
- Symbiotic relationship between developments in computer programming skills and hacking
- Introduction to understanding a popular programming language (Python)

## Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).



## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (20-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assignment: Choice of two:

- a) Identify and explain how you would host organizational databases on the Cloud? How would you ensure that your Cloud-hosted databases were set to the highest possible standards of security? (Maximum 1,500 words.)

Or:

- b) How and why is Python programming language used successfully by Black Hat Hackers? Apply your answer to the real world, by way of exploring one case study scenario, whereby Python was used to maliciously 'attack' a system. (Maximum 1,500 words.)

## Suggested Resources

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](https://docs.oracle.com/cd/E11882_01/network.112/e36292/toc.htm)

Mark Lutz (2013) *Learning Python* (5<sup>th</sup> Ed.) Newton: USA, O'Reilly Media

## Unit CSEC04: Incident Response, Investigations and Forensics

Unit code: T/617/1132

RQF level: 4

### 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

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
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

## Indicative Content

- CERTS: how to build the right teams to respond
- Incident Response: structure, people, scope
- Reporting and recording IR activity
- Aligned disciplines: Business Continuity Management, Disaster Recovery and Crisis Management
- Legal and ethical principles and computer network investigations
- Principles of forensic science and digital forensics
- Evidence handling: concepts, protocols and tools

## Delivery Guidance:

This 20-credit unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres to deliver. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (20-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Produce a computer network INCIDENT RESPONSE PLAN for a large globally-dispersed business or organisation of more than 5,000 terminal users – 2000 words.

## Suggested Resources

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* (3<sup>rd</sup> Ed.), McGraw Hill Education

## Unit CSEC05: Security Strategy: Laws, Policies and Implementation

Unit code: A/617/1133

RQF level: 4

### 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 and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
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	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

risk management	
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

### Indicative Content

- Strategic management, and how it applies to cyber security environments
- Cyber security policies and planning
- Legal, regulatory and standards bodies
- Training and further development – standards and training
- Future legal and technical environment and a range of national and international approaches
- Design a security audit

### Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (20-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Develop a slide presentation with accompanying notes on how the legal and political environment can impact the cyber security functions within your business operating environment. What laws, regulations and standards could be of **particular significance** to your cyber security policies and operations in your business? (maximum 1,500 words.)

## Suggested Resources

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](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework)

Touhill, G, and Touhill, T.J (2014) *Cyber Security for Executives*, New York: Wiley

## Unit CSEC06: ELECTIVE: Cyber Security Threats and Risks: Banking and Finance

Unit code: F/617/1134

RQF level: 4

### 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 and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
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 cryptocurrencies connect to underpinning financial services architecture	4.1 Evaluate emerging trends and threats from cryptocurrency-related attacks by cyber criminals



## Indicative Content

- Threats and risks to Banking and Finance institutions and processes
- Case studies in banking and finance cyber-crime: TinyBanker Trojan (tinba), Zeus, Carbanak, inter alia
- Legal, regulatory requirements and standards
- The Payment Card Industry Data Security Standards suite
- Cyber security and cryptocurrencies

## Delivery Guidance:

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for students to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (20-credit) units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Write an investigative report into the methods used by cyber-criminals to attack Financial Institutions. Provide a Courses of Action report to an imagined executive Board at a bank in order to reduce cyber-crime attacks against the institution? (2,000 words)

### Suggested Resources:

British Bankers Association (2014) *The Cyber Threat To Banking: A Global Industry Challenge*, accessed at: [https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110\\_Cyber\\_report\\_May\\_2014\\_WEB.pdf](https://www.bba.org.uk/wp-content/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](https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf)

## Unit CSEC07: ELECTIVE: Cyber Wars

Unit code: J/617/1135

RQF level: 4

### Aim

In this unit the learner will look at the emerging cyber offensive and defensive strategies of nation states that reportedly engage in what is called 'cyber war' or 'information warfare'.

What nation-state governments have the most advanced cyber capabilities? How might they be used to defend or attack an institution, group or infrastructure? Why is this knowledge important for cyber security practitioners based within businesses? As part of this unit learners will analyse geopolitical considerations in relation to cyber security incidents and also explore the direct, likely implications, for their business organisations, and surrounding Critical National Infrastructure (CNI), that might get caught up in widescale disruption and long-term power outage.

### Learning and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand how nation states are potentially engaged in cyber defence and offensive capability strategy	1.1 Explain the terms 'geopolitics' and 'state-sponsored/sanctioned' as they apply to considerations for information security 1.2 Assess the threats and risks to businesses from emerging nation-state cyber 'warfare' capabilities
2 Understand the motivations and causes behind nation-state-linked cyber-attacks and breaches	2.1 Explain the difficulty in attributing cyber-attacks to state sponsored actions 2.2 Analyse how 'plausible deniability' benefits some countries
3 Understand how private sector industry has been targeted by potentially state-sanctioned cyber-crime groups and/or armies	3.1 Assess vulnerable sectors and types of business 3.2 Analyse how company behaviour and culture could increase risk from external attacks 3.3 Evaluate a successful investigative and risk management strategy to lessen an organisation's risk profile
4 Understand how CNI has been targeted by state-backed cyber-crime groups and/or armies	4.1 Assess how attacks on Critical National Infrastructure can impact a business's access to its information systems 4.2 Assess measures to lessen an organisation's risk profile

## Indicative Content

- What do we mean by cyber or information 'warfare' and where might such heightened risks exist?
- Strategy, methods and motivations behind state-sponsored/encouraged cyber conflict/war
- Concepts and approaches to geopolitics
- Case studies in business communities and private sector responses
- Case studies in CNI and sector responses
- Remediation and DR strategies for mass-disruption scenarios

## Delivery Guidance:

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by QUALIFI to all centres. This learner-support information will be presented within clearly separated tabs, including:

*Unit Content:* Actual learning content broken down into weekly stages with a reflective learning end-section

*Video-shelf:* Unit content and additional information provided by the course leader via video

*Podcasts:* Podcasts are broadcast by the GlobalCyberAcademy.com and cover the Learning Outcomes of each unit.

*E-library:* Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list

*Assignment Instructions:* Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing, as well as making presentations

*Discussion Board:* Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

## Assessment Guidance

Each unit in this qualification is worth **20 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the six (20-credit) units, every learners will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will be by way of completing a formative exercise/s throughout the unit.

Summative Assessment: Write an investigative report into the methods used by alleged state-sanctioned cyber-criminals to attack another country's banking and finance industry. Provide a Courses of Action report to an imagined Executive Board at a bank in order to prepare that Board for a large-scale attack that might also include supporting Critical National Infrastructure. What business security prevention measures, and business resilience measures, do you advocate should be put in place over the next 12 months? (2,000 words)

## Suggested Resources:

Clarke, R. and Knake, R., (2012) *Cyber War: The Next Threat To National Security And What To Do About It*, New York: Ecco

Nance, N (2016) *The Plot To Hack America*, New York: Skyhorse Publishing

Townsend, K., (2017) The Increasing Effect of Geopolitics on Cyber Security, accessed via Wombat Security Technologies on 21/01/2018 at: <http://www.wombatsecurity.com/in-news/news/increasing-effect-geopolitics-cybersecurity>