Level 3 Diploma in Cyber Security Management and Operations

Level 4 Diploma in Cyber Security

Level 5 Diploma in Cyber Security

Specification (For Centres)

October 2023

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.

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
About QUALIFI 5
Why Choose QUALIFI Qualifications? 5
Support for the Qualification Development 5
Equality and Diversity 5
Qualification Titles and Accreditation Number 6
Qualification Purpose, Aims and Learning Outcomes 6
Purpose 6
QUALIFI Level 3 Diploma in Cyber Security Management and Operations 7
QUALIFI Level 4 Diploma in Cyber Security. 8
QUALIFI Level 5 Diploma in Cyber Security 9
Aims of the Diplomas 11
QUALIFI Level 3 Diploma in Cyber Security Management and Operations 11
QUALIFI Level 4 Diploma in Cyber Security 12
QUALIFI Level 5 Diploma in Cyber Security 12
Learning Outcomes of the Diplomas 13
QUALIFI Level 3 Diploma in Cyber Security Management and Operations 14
QUALIFI Level 4 Diploma in Cyber Security 14
QUALIFI Level 5 Diploma in Cyber Security 15
Delivering the Qualifications 16
External Quality Assurance Arrangements 16
Learner Induction and Registration 16
Entry Criteria 17
Recognition of Prior Learning 18
Data Protection 18
Learner Voice 18
Professional Development and Training for Centres 19
Progression and Links to other QUALIFI Programmes 19
Qualification Structure and Requirements 20
Units, Credits and Total Qualification Time (TQT) 20
Rules of Combination for QUALIFI Diplomas 21
Level 3 Diploma in Cyber Security Management and Operations 21
Level 4 Diploma in Cyber Security 22
Level 5 Diploma in Cyber Security 23
Achievement Requirements 24
Awarding Classification/Grading 24

Assessment Strategy and Methods 25
Appendix 1: Unit Descriptors 27
Level 3 Diploma in Cyber Security Management and Operations 42
Unit CSM01: Threat and Risk: Expecting the Unexpected 42
Unit CSM02: Network Architecture, Communications and Protocols 45
Unit CSM03: Mobile Device and Data Risks 48
Unit CSM04: Investigations and Incident Response 51
Unit CSM05: Solutions: Future-Proofing your Business 54
Unit CSM06: EU GDPR and Data Security 57
Level 4 Diploma in Cyber Security 60
Unit CSEC01: Cyber Security Threat and Risk 60
Unit CSEC02: Network Security and Data Communications 63
Unit CSEC03: Database Security and Computer Programming 66
Unit CSEC04: Incident Response, Investigations and Forensics 69
Unit CSEC05: Security Strategy: Laws, Policies and Implementation 72
Unit CSEC06: ELECTIVE: Cyber Security Threats and Risks: Banking and Finance 75
Unit CSEC07: ELECTIVE: Cyber Wars 78
QUALIFI Level 5 Diploma in Cyber Security 81
Unit DSC01: Cryptography 81
Unit DCS02: Digital Investigations and Forensics 84
Unit DSC03: Communications and Incident Management 87
Unit DSC04: Strategic Leadership 90

About QUALIFI

QUALIFI is recognised and regulated by Ofqual (Office of Qualifications and Examinations Regulator). Our Ofqual reference number is RN5160. Ofqual regulates qualifications, examinations, and assessments in England.
As an Ofqual recognised Awarding Organisation, QUALIFI is required to carry out external quality assurance to ensure that centres approved for the delivery and assessment of QUALIFI's qualifications meet the required standards.

Why Choose QUALIFI Qualifications?

QUALIFI qualifications aim to support learners to develop the necessary knowledge, skills and understanding to support their professional development within their chosen career and or to provide opportunities for progression to further study.
Our qualifications provide opportunities for learners to:

- apply analytical and evaluative thinking skills
- 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.

Support for the Qualification Development

During the development of this qualification QUALIFI consults with a range of employers, providers, and existing centres where applicable, to ensure rigor, validity, and demand for the qualification and to ensure that the development considers the potential learner audience for the qualification and assessment methods.

Equality and Diversity

QUALIFI's qualifications are developed to be accessible to all learners who are 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 teaching and learning are free from any barriers that may restrict access and progression.

Learners with any specific learning need should discuss this in the first instance with their approved centre who will refer to QUALIFI's Reasonable Adjustment and Special Consideration Policy.

Qualification Titles and Accreditation Number

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

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

QUALIFI Level 5 Diploma in Cyber Security 603/4139/7)

Qualification Purpose, Aims and Learning Outcomes

Purpose

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.

QUALIFI Level 5 Diploma in Cyber Security

The rationale of the Diploma 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. It is also to provide a pathway via learner credits and potential direct entry into related Level 6 Cyber Security and/or Risk Management Degree programmes.

All QUALIFI programmes create learning that advances the thought leadership of organisations, offering conceptual and practical insights that are applicable in the companies of today and tomorrow.

Furthermore, we look to develop the cyber security team leaders, managers and leaders of the future through the creation and delivery of learning appropriate for that industry.

The qualification will:

- advanced levels of higher education learning
- prepare learners for employment; and
- support a range of senior IT and Digital, Data and Security roles in the workplace.

By 2019, it is predicted that cyber security breaches will cost the global economy $2 Trillion per annum (Forbes). Back in 2015, insurance firm Lloyd's of London assessed cyber breaches to have cost international commerce some $400bn. This multiplication of the economic value of threat and risk (500% over four years) is likely to continue following a wave of mega data breaches, state-sponsored attacks, bespoke malware refinement, and the mainstreaming of IoT (50 billion web-enabled devices: Cisco) and cryptocurrencies. The cyber security market sector has now reached at least $100bn in value (GlobalCyberAcademy.com: 2018). As an exemplar, the median annual wage for Information Security professionals was some $87,000 in the USA by 2012. This is expected to rise by 37% by 2022 (*Bureau of Labor Occupational Handbook 2014-15*).

This Level 5 qualification is potentially unique because it is about 'cyber security' as a workplace management discipline. It is therefore a semi-technical qualification that examines technical cyber security measures as well as the management, project management and leadership skills required to organise internal and external business responses to major incidents (or the threat of such).
Due to the huge economic risks to businesses, sectors, as well as global regions, from specific and dynamic forms of threat vectors, this course programme will provide solid business management and leadership education (including disaster management, project management and business continuity management) within the context of the digital tech and cyber security threat environment. The course programme is designed and delivered by a mix of academics from Business Schools and Security Management teaching roles.

This Level 5 course is especially designed for existing or aspiring organisational executives and leaders who are tasked with responsibility for business resilience, information security, safe technological innovation, safe and secure change management, HR planning and physical risk management, professionals.

The course is flexible and online. It is easily able to be blended. The programme utilises many case studies from business and public-sector organisations and embeds isomorphic learning into its technical and management education. The programme is particularly suited for those who are already in work. Or those who are seeking to develop a structured management competency in information security, risk management and organizational resilience.

This course particularly suits students who work for large multinational firms, international organisations or widely distributed governmental bodies and agencies. Often our 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, as well as those responsible for the confidentiality, integrity and availability of company data processes. 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 first complete the Qualifi Level 3 Diploma in Cyber Security Management and Operations, then scale up to the Level 4 Diploma in Cyber Security, before enrolling onto this course programme. Learners seeking to enter a university degree top-up programme will be required to have successfully completed our Cyber Security Diplomas at Levels 4 and 5, and attain the respective 240 learning credits, before their application for a Level 6 Top-Up application with a university can be considered.

The qualification will identify and evaluate practical ways to safely and securely protect people and organisations from cyber-attacks, data breaches and the consequential impacts. This will be done by accessing and researching a wide range of open-source information: websites, specialist books, journals, manuals, news articles, guidance, International Standards, court documents and other materials. Videos, audio, course content, informal exercises and formal assignments will all be provided by the course tutor team.

Aims of the Diplomas

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.

QUALIFI Level 5 Diploma in Cyber Security

This Level 5 Diploma provides the opportunity for individuals to develop a more advanced career in a specific area of business or public organisations by developing analytical knowledge and deeper understandings of several core cyber security operational domains. The course will also provide core information security technical and generic management and leadership teaching. Much of this teaching will be directly relevant to learners moving forward into Information Security Management technical qualifications at the higher-end of the industry market, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

At key points, in each unit, learners will be asked to use their own equipment to practise using, and conduct live exercises on, technical IT hardware and software platforms and apps, including Virtual Machines, Linux OS, as well as working beyond the GUI (Graphical User Interface) and into their own Command Lines.

Learners studying this course via the Global Cyber Academy (globalcyberacademy.com), our Approved Learning Centre, will have free access to its many cyber security industry events, videos, audio and e-library.

This course's core aims are:

1. To equip individuals with the knowledge, understanding and skills required for success in information-security-related employment
2. To enable progression into a university approved Level 6 Degree award
3. To provide 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. To develop learners' ability to contribute positively to good and ethical practice in technology and risk management environments, through effectively utilising the practical and theoretical knowledge and skills gained.

To develop skills and techniques, personal qualities and attributes essential for successful performance in working life and thereby enabling learners to make a positive contribution to their employment and therefore enhance their prospects for promotion and remunerative advancement.

Learning Outcomes of the Diplomas

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.

QUALIFI Level 5 Diploma in Cyber Security

Learners studying for the Level 5 Diploma in Cyber Security 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), hardware and software, with a proficient or developed competence
2. Understanding: the ability to think independently and solve potential overarching cyber security issues within a business or organisation
3. Apply subject knowledge and understanding to address familiar and unfamiliar problems in the cyber security and digital risk management domains within their workplace and/or sector
4. Recognise 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
5. An appreciation of the interdisciplinary and interdependent nature of cyber security within wider business and service provision, and broader operating environments and supply chains
6. 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
7. To develop transferable skills and knowledge – including in project management, business continuity management crisis management, disaster recovery and management and incident response - which will enable individuals to meet the requirements of, and successfully manage/lead, major business incidents
8. To motivate individuals to progress to further professional development and advancement through future study or as part of their chosen career
9. To 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.
10. To engender positive digital citizenship, inculcating an ethos of understanding responsibilities and exercising personal and organisational ‘rights’ in an ethical, responsible and sustainable manner

Delivering the Qualifications

External Quality Assurance Arrangements

All centres are required to complete an approval process to be recognised as an approved centre. Centres must have the ability to support learners Centres must commit to working with QUALIFI and its team of External Quality Assurers (EQAs). Approved Centres are required to have in place qualified and experienced tutors, all tutors are required to undertake regular continued professional development (CPD).

Approved centres will be monitored by QUALIFI External Quality Assurers (EQAs) to ensure compliance with QUALIFI requirements and to ensure that learners are provided with appropriate learning opportunities, guidance, and formative assessment.

QUALIFI's guidance relating to invigilation, preventing plagiarism and collusion will apply to centres.

QUALIFI, unless otherwise agreed:

- sets all assessments;
- moderates' assessments prior to certification;
- awards the final mark and issues certificates.

Learner Induction and Registration

Approved Centres should ensure all learners receive a full induction to their study programme and the requirements of the qualification and its assessment.

All learners should expect to be issued with the course handbook, a timetable and meet with their personal tutor and fellow learners. Centres should assess learners carefully to ensure that they are able to meet the requirements qualification and that if applicable appropriate pathways or optional units are selected to meet the learner's progression requirements.

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 to support them in making the necessary qualification and unit choices. During recruitment, approved centres need to provide learners with accurate information on the title and focus of the qualification for which they are studying.

All learners must be registered with QUALIFI within the deadlines outlined in the QUALIFI Registration, Results and Certification Policy and Procedure.

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 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.

QUALIFI Level 5 Diploma in Cyber Security

- learners who possess qualifications at Level 4 and/or;
- learners who have some technical and risk management work experience in a computing or security business environment and demonstrate ambition with clear career goals;
- learners who possess a Level 5 qualification in another discipline and want to develop their careers in cyber security and/or risk management.

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.

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 *Recognition of Prior Learning Policy*.

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 and may be made available to our regulators. 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

Learner Voice

Learners can play an important part in improving the quality through the feedback they give. In addition to the on-going discussion with the course team throughout the year, centres will have a range of mechanisms for learners to feed back about their experience of teaching and learning.

Professional Development and Training for Centres

QUALIFI support its approved centres 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 learner-centred learning and teaching approaches
- building in effective and efficient quality assurance systems.

Please contact us for further information.

Progression and Links to other QUALIFI Programmes

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.

Learners completing the **QUALIFI Level 5 Diploma** can progress to:

- (Pending a successful application to our Partner institution) a Level 6 University Degree (Top-Up) course
- directly into employment in an associated profession.

Qualification Structure and Requirements

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 QUALIFI Level 5 Diploma in Cyber Security is a Level 5 qualification made up of **four units** equating to 120 credits. All units are 30 credits in value. Each 30-credit unit approximates to a TQT of 300 hours incorporating 150 hours of GLH. 120 credits equates to 1200 hours of TQT.

Total Qualification Time (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.

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, live webinars, telephone tutorials or other forms of e-learning supervised by a tutor in real time. Guided learning includes any supervised assessment activity; this includes invigilated examination and observed assessment and observed work-based practice.

Rules of Combination for QUALIFI Diplomas

Level 3 Diploma in Cyber Security Management and Operations

There are six 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
T/617/1163	Threat and Risk: Expecting the Unexpected	3	10	100	60
F/617/1165	Network Architecture: Communications and Protocols	3	10	100	60
J/617/1166	Mobile Device and Data Risks	3	10	100	60
R/617/1168	Investigations and Incident Response	3	10	100	60
R/617/1171	Solutions: Future-Proofing your Business	3	10	100	60
Y/617/1172	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
T/617/1129	Cyber Security Threat and Risk	4	20	200	120
K/617/1130	Network Security and Data Communications	4	20	200	120
M/617/1131	Database Security and Computer Programming	4	20	200	120
T/617/1132	Incident Response, Investigations and Forensics	4	20	200	120
A/617/1133	Security Strategy: Laws, Policies and Implementation	4	20	200	120
Unit Reference	**Elective Units**	**Level**	**Credit**	**TQT**	**GLH**
F/617/1134	Cyber Security Threats and Risk: Banking and Finance	4	20	200	120
J/617/1135	Cyber Wars	4	20	200	120

Level 5 Diploma in Cyber Security

The QUALIFI Level 5 Extended Diploma in Cyber Security comprises four units in total:

The Diploma requires 4 Mandatory Units

Unit Reference	Mandatory Units	Level	Credits	TQT	GLH
J/617/4634	Cryptography	5	30	300	150
L/617/4635	Digital Investigations and Forensics	5	30	300	150
R/617/4636	Communications and Incident Management	5	30	300	150
Y/617/4637	Strategic Leadership	5	30	300	150

Achievement Requirements

Learners must demonstrate they have met all assessment criteria for all units to achieve this qualification. QUALIFI will issue certificates to all successful learners via their registered centres.

Awarding Classification/Grading

All unit grading is shown on the qualification transcript.

QUALIFI Level 2 Diploma Business Beginners in Cyber Security is pass/fail. Pass mark is 40% for each unit.

QUALIFI Level 3 Diploma in Cyber Security Management and Operations is pass/fail. Pass mark is 40% fo reach unit.

Level 4 and Level 5 qualifications are graded:

Fail - 0-39%
Pass - 40%-59%
Merit - 60% - 69%
Distinction 70%+

All units will be internally assessed through written assignment, internally marked by the QUALIFI approved centre and subject to external quality assurance by QUALIFI.

Assessment Strategy and Methods

QUALIFI will provide assessments for each unit of this qualification. These tasks will address all learning outcomes and related assessment criteria, all of which must be demonstrated/passed in order to achieve the qualification. To achieve a pass for each of the units, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

The assessment tasks will require learners to draw on real organisational information or case studies 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, encourage learners to draw on work-place opportunities to undertake research and investigation to support their learning.

Learners' assessments will be marked internally by the approved centre and will be subject to external moderation by QUALIFI prior to certification.

Qualifi may provide summative assessments that cover the learning outcomes and assessment criteria. In addition formative assessments may be offered.

1: Formative Assessment

Formative assessment is an integral part of the assessment process, involving both the tutor/assessor and the learner about their progress during the course of study. Formative assessment takes place prior to summative assessment and focuses on helping learners to reflect on their learning and improve their performance and does not confirm achievement of grades at this stage.

The main function of formative assessment is to provide feedback to enable learners to make improvements to their work. This feedback should be prompt so that it has meaning and context for learners and time must be given following the feedback for actions to be complete. Feedback on formative assessment must be constructive and provide clear guidance and actions for improvement. All records should be available for auditing purposes as we may choose to check records of formative assessment as part of our on-going quality assurance. Formative assessments will not contribute to the overall mark of the units.

2: Summative Assessment

Summative assessment is used to evaluate learner competence and progression at the end of a unit or component. Summative assessment should take place when the assessor deems that the learner is at a stage where competence can be demonstrated.

Learners should be made aware that summative assessment outcomes are subject to confirmation by the Internal Verifier and External Quality Assurer (EQA) and thus is provisional and can be overridden. Assessors should annotate on the learner work where the evidence supports their decisions against the assessment criteria. Learners will need to be familiar with the assessment and grading criteria so that they can understand the quality of what is required.

Formative Assessment	Summative Assessment
used during the learning process	used at the end of the learning process
provides feedback on learning-in-process	evaluates achievement against learning outcomes and assessment criteria
dialogue-based, ungraded	graded pass / refer

Evidence of both formative and summative assessment MUST be made available at the time of external quality assurance – EQA.

Please contact Qualifi for more information.

Appendix 1: Unit Descriptors

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 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 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 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 investigative 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 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 (3rd 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

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 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 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.allenovery.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 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* (2nd. 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 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 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

Mark Lutz (2013) *Learning Python* (5th 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 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 (3rd 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	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

	security planning and digital 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 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

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 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

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

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 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

QUALIFI Level 5 Diploma in Cyber Security

Unit DSC01: Cryptography

Unit code: J/617/4634
RQF level: 5

Aim

The process of encrypting and decrypting information forms the basis of much computer, device and network security. Cryptography is designed and used to protect the confidentiality, integrity and authenticity of information. From the very beginnings of computing, and throughout the industry's evolution, the establishment of policies, guidelines and laws has shaped the disciplines of information security and organisational resilience in profound and, often, unintended, ways.

In this unit learners will be introduced to the concept and history of cryptography, and its subdisciplines (including cryptology), and how cyber-enabled networks and devices have their communications security underpinned by cryptographic methods and sector standards. Learners will explore methods of attack, including side-channel, additional encryption methods and escrow principles and key.

Learners will look at how businesses can deploy encryption to enhance their information security approaches.

Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

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 cryptographic principles and modes	1.2 Define the concept and application of cryptography 1.3 Explain symmetric and asymmetric modes and approaches 1.4 Assess how cryptographic methods and standards underpin the communications security of cyber-enabled networks and devices
4 Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption	4.1 Explain the key principles of the related standards, regulations and laws and why they are in place 4.2 Assess the consequences for organisations and individuals of non-compliance with these standards, regulations and laws

5 Design an encryption plan and courses of action for a given organisation	3.1 Explain the methods of attack used to target encrypted data 3.2 Assess the additional encryption methods available 3.3 Explain the key principles of escrow and recovery 3.4 Explain the importance of having robust encryption arrangements within IT systems 3.5 Evaluate the existing encryption arrangements 3.6 Design an encryption plan to meet the needs of a given organisation, with recommended courses of actions

Indicative Content

-The science of crypto

-Cipher types

-Symmetric and asymmetric

-Methods of attack

-Standards, regulations, legal domains

-Key escrow and recovery

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.

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 will be worth **30 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 module assessment point.

During each of the four 30-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 by way of completing a formative exercise/s throughout the unit.

Summative Assignment: CONSULTANCY REPORT - Write a company or business report reviewing a) existing encryption arrangements within the IT system, and b) offering a Courses of Action group of recommendations for the company's CISO (3000 words).

Suggested Resources

Gordon Corera (2015) Intercept: The Secret History of Computers and Spies (London: W&N), available at: **https://www.amazon.co.uk/Intercept-Secret-History-Computers-Spies/dp/0297871730**

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

Lawrence Miller and Peter Gregory (2018) CISSP For Dummies (USA: John Wiley & Sons), available at: **https://www.amazon.co.uk/CISSP-Dummies-Computers-Lawrence-Miller/dp/0470537914**

Twitter - @GlobalCAcademy
-@bruceschneier

Unit DCS02: Digital Investigations and Forensics

Unit code: L/617/4635
RQF level: 5

Aim

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

In this unit learners will examine the requirements for digital investigations including team formations and tools, understanding the prospects of recovering information, gathering evidential data (including from mobile and IoT devices), safeguarding evidential integrity, as well as the complexity and challenges of storing and presenting evidence within legal environments.

Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

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 principles of digital investigations	1.2 Explain the investigation lifecycle from initiation to conclusion 1.3 Explain how a 'digital' domain investigation is organised and managed
2 Apply the types of tool that support professional digital investigations at a strategic level	3.1 Analyse the range of tools that assist digital investigations in different situations 3.2 Select the appropriate tools to carry out a digital investigation for a given situation, justifying the selection

3. Plan for an investigations and forensics teams	3.1 Explain the types of skills required to undertake a variety of investigations and forensic-related work 3.2 Explain dynamics of forming and integrating digital investigation teams and geographically distributed and dispersed investigations and teams 3.3 Develop a plan for the formation of an investigation and forensics teams
4. Understand the importance of safeguarding evidential integrity in digital investigations	4.1 Explain how evidence can be retrieved from mobile devices and IoT devices 4.2 Analyse how evidential integrity is safeguarded during digital investigations 4.3 Assess how evidence is stored and presented within legal environments

Indicative Content

-Requirement for digital investigations

-Understanding evidential data and prospects of recovery

-Mobile, portable and apps in DI

-Evidential integrity and chain of custody

-Processes and timelines

-Legal domains and cross examination

-Management and budgeting

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 Qualify 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.

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 will be worth **30 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 four 30-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 by way of completing a formative exercise/s throughout the unit.

Summative Assignment: (REPORT) Conduct an investigation into a suspected mega breach of an Internet Services Provider that has lost the login credentials for 150,000 business clients.
Questions:

1. Explain to their CEO the investigative stages that you have passed through and why each stage was necessary. (1000 words)
2. Imagine that your suspicions are now focused on an internal leak, perhaps a group or couple of employees located offsite in your 'hot' disaster recovery centre. Identify and explain what tools you might need to acquire to prove your case further, and estimate the costs (1000 words)
3. Explain and evaluate how you will securely store the evidence until it is handed over to the local police. (1000 words)

Suggested Resources

Bilton, N. (2017) American Kingpin: The Epic Hunt for The Criminal Mastermind Behind the Silk Road (Portfolio)

Sachowski, j. (2018) *Digital Forensics and Investigations: People, Processes and Technologies* (CRC Press)

Sikorski, M and Honig, A., (2012) *Practical Malware Analysis* (No Starch Press)

Unit DSC03: Communications and Incident Management

Unit code: R/617/4636
RQF level: 5

Aim

The professional and lawful response to managing an incident can be the difference between company survival or otherwise. Poor responses to major incidents, including mega data breaches, have significantly damaged organisational reputations and financial performance. Significantly mismanaging a cyber incident can result in catastrophic personal and organisational consequences. Such business 'impacts' are covered in-depth within our Threat and Risk units at Levels 2, 3 and 4. and will be explored during this Level 5 unit as part of the contextual case-study learning, and isomorphic reflections, that are central to this unit.

In this unit learners will explore the types of site, personnel and equipment required in relation to planning for Incident Management and forming an organisational CERT team (Computer Emergency Response Team). They will then explore the core sub-disciplines and side-disciplines of Cyber Incident Management: Disaster Recovery, Business Continuity Management and Crisis Management. Learners will discuss the importance of the business organisational requirement for skilled and planned communications to operate in combination with advanced and developed management responses and strategy.

Learners will develop an understanding of the security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

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 physical and human resources required to manage a major suspected cyber security incident	1.1 Explain site-set-up, staffing and organisational arrangements for major suspected cyber-related incidents
2 Apply Business Continuity Management to major incident planning and response	2.1 Assess how Business Continuity Management can be aligned and integrated into a suspected cyber-enabled incident 2.2 Explain the people, assets and processes required within a Business Continuity Plan
3 Understand how Disaster Recovery and Crisis Management	3.1 Assess how DR and CM strategies and tactics in relation to a suspected major cyber-enabled incident

are integrated into a suspected major cyber-enabled incident	3.2 Explain the components of good practice in DR and CM plans
4 Evaluate the potential impact of NOT planning crisis communications and incident response	4.1 Evaluate the isomorphic lessons from major cyber breaches and company shutdowns 4.2 Analyse communications approaches and perceived failures in cases of catastrophic business loss related to IT systems failure or attack 4.3 Justify recommendations that would support a cyber-resilient approach

Indicative Content

-Equipment and location requisites

-Disaster Recovery and Management

-Business Continuity Management

-Crisis Management

-Cyber Resilience: including considerations of future-proofing and disruptive technology

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.

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 will be worth **30 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 module assessment point.

During each of the four 30-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 by way of completing a formative exercise/s throughout the unit.

Summative Assignment: ESSSAY – Identify and explain a case study that could be translated as a weak organisational response to a major cyber-security incident. Evaluate how the organisation responded and provide recommendations that would support a more cyber-resilient approach over the next five years. (3000 words)

Suggested Resources

Austin, L and Jin, Y (2017) *Social Media and Crisis Communication* (Routledge)

Richard Bingley (2015) *The Security Consultant's Handbook* (Ely: IT Governance Press), available at: **https://www.itgovernance.co.uk/shop/product/the-security-consultants-handbook**

Heng, G.M (2017) A Manager's Guide to Business Continuity Incidents for Cyber Security Incidents, The Business Continuity Management Institute, available at: **https://www.bcm-institute.org/product/a-managers-guide-to-business-continuity-management-for-cybersecurity-incident-response/**

Unit DSC04: Strategic Leadership

Unit code: Y/617/4637
RQF level: 5

Aim

In order for an organisation to be more cyber secure, leadership across employee and stakeholder networks is required to be delivered by the C-Suite. However, what happens if the C-Suite either doesn't listen or doesn't understand the Tier One threat posed by information security vulnerabilities.

In this unit learners will develop an understanding of the key features of tech leadership and performance management. Learners will evaluate strategic leadership and management approaches, within a tech sector setting, and what it means to be a 'senior level influencer'.

Learners will also develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP). The unit is also highly applicable to learners who are considering taking an MBA, or MBA in Cyber Security, at a later date or who looking to advance into senior management roles within their organisation or sector.

Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
2 Understand the role senior leaders and strategic leadership	2.1 Explain the key roles and responsibilities of senior leaders in a tech sector setting 2.2 Assess how strategic leadership and core goal-setting can enable stronger security cultures
2 Evaluate the management streams and performance monitoring mechanisms that relate to information security	2.1 Explain the importance of integrating management and operational programmes in relation to optimum levels of performance and cyber resilience 2.2 Anlayse the performance monitoring mechanisms in place to protect information security 2.3 Assess how cultural and diversity-related complexities impact on management and performance monitoring
4 Understand how threat and risk identification and management is integrated	4.1 Evaluate risk management and threat identification within the context of wider corporate strategy, responsibilities and governance 4.2 Explain the impact of poor or ineffective C-Suite understanding and direction

into C-Suite considerations and governance	4.3 Assess the importance of business ethics and leadership in business values, including within end-user environments of ICT systems
4 Understand how data protection legislation impacts considerations of strategy-setting and strategic leadership	4.1 Evaluate how major data protection laws, impact on C-Suite strategic level decision making and strategy setting 4.2 Assess the consequences for individuals and organisations of non-compliance with this legislation

Indicative Content

-Strategic leadership

-Strategic management, project management and configuration management

-Threat and risk management: global business environments

-Cultural complexity

-Ethics, compliance and governance

Delivery Guidance

This 30-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. 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.

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 will be worth **30 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 module assessment point.

During each of the four 30-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 by way of completing a formative exercise/s throughout the unit.

Summative Assessment: REPORT: Identify an organisation that recently experienced a mega data breach.

1. Prior to the event, what was the style of leadership, the corporate strategy, the goals of that organisation? (800 words)
2. Prior to the event, analyse how well the company/organisation was perceived by the market and its shareholders to be performing. (800 words)
3. Following the data breach, in your assessment, what laws in relation to the major incident (or related activities) is the company guilty of breaching? (800 words)
4. Following the data breach, in your assessment, how well is the company performing? (800 words)
5. Following the data breach, to what extent has the company/organisational strategic leadership been successful? (800 words)
   (Total: 4000 words)

Suggested Resources

Henderson, G. (1994) Cultural Diversity in the Workplace, Praeger

'Krebs on Security' cyber security and news blog accessed at: https://krebsonsecurity.com/

Rumelt, R (2017) *Good Strategy: Bad Strategy: The difference and why it matters* (Profile Books)