

SEVERN BUSINESS COLLEGE

Qualifi Level 5 Extended Diploma in Cyber Security

Course Handbook

Qualification
Qualifi Level 5 Extended Diploma in Cyber Security

Ofqual Number
610/3296/7

Level
5

Total Qualification Time
2400

Credit Value
240

Aim of the Course
This Level 4 programme provides the opportunity for individuals to develop a more advanced career in a specific area of business or public organisations by developing analytical knowledge and deeper understandings of several core cyber security operational domains. The course will also provide useful generic management and leadership teaching at key points in order to help learners to build essential support from within the business for their cyber security work including (but not limited to): Project Management, Risk Management and Business Case writing skills.
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).

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

Course Structure

Qualifi Level 5 Extended Diploma in Cyber Security			
Unit number	**Mandatory Units**	**Unit level**	**Unit credit**
T/617/1129	Cyber Security Threat and Risk	4	20
K/617/1130	Network Security and Data Communications	4	20
M/617/1131	Database Security and Computer Programming	4	20
T/617/1132	Incident Response, Investigations and Forensics	4	20
A/617/1133	Security Strategy: Laws, Policies and Implementation	4	20
F/617/1134	Cyber Security Threats and Risk: Banking and Finance	4	20
J/617/4634	Cryptography	5	30
L/617/4635	Digital Investigations and Forensics	5	30
R/617/4636	Communications and Incident Management	5	30
Y/617/4637	Digital Leadership	5	30

Assessment Grades

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

UNIT SPECIFICATIONS

Unit Title
Cyber Security Threat and Risk

Level
4

Learning Time Hours
200

Credit Value
20

Unit aim
Cyber security breaches cause significant personal and organisational damage and pose a clear and present risk to business profitability and resilience. Forbes, the business magazine, estimates that the annual cost of cyber-crime might reach (or surpass) $2Trillion by 2019. At a ground-level, Cyber security breaches are causing business insolvencies and posing challenges to employee safety and wellbeing. In this unit the learner will be introduced to a variety of threats and risks emanating from the cyberspace. The unit will look at various methods of attack and will use case studies to analyse various threat vectors, including Malware, Botnets and Trojans. The unit will introduce and explain various models of measuring threats, risks and impacts. Including, those proposed and recommended by a range of information security standards published by the International Standards Organisation and US NIST (National Institute of Standards and Technology). Using a well-documented 'real-world case study', the learner will investigate and examine the business impact of a recent mega data breach.

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

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

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 SPECIFICATIONS

Unit Title
Network Security and Data Communications

Level
4

Learning Time Hours
200

Credit Value
20

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

Learning outcomes and assessment criteria

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

Learning Outcome	Assessment Criteria
1. Understand how computers and digital devices communicate with one another over a network	1.1 Analyse the core vulnerabilities within a network environment and an online environment 1.2 Explain how the emergence of security thinking and tools can benefit a network environment
2. Understand, at a strategic level, how computer networking, web applications and software can be exploited.	2.1 Evaluate the link between network architecture and security engineering concepts
3. Understand methods of security prevention and systems hardening	3.1 Evaluate internal risks and exposure 3.2 Evaluate available process and physical defences against malicious network intrusions
4 Understand key network security and systems resilience tools, terminology and models	4.1 Explain how key security concepts can be applied in a large and distributed organisation 4.2 Assess how key factors are applied to enhance and embed an holistic approach to network and systems resilience

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 SPECIFICATIONS

Unit Title

Database Security and Computer Programming

Level

4

Learning Time Hours

200

Credit Value

20

Unit aim

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

Learning outcomes and assessment criteria

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

Learning Outcome	Assessment Criteria
1. Understand the broad range of information security controls to protect databases	1.1 Explain security risks in database systems 1.2 Assess the effectiveness of information security concepts and tools in protecting databases
2. Understand types of database categories of control	2.1 Explain database terminology and categories of control
3. Understand the underpinning concepts and models of cloud-based	3.1 Explore the functionality of database tools available to Data Owners, Custodians, Incident Responders and Investigators

storage solutions	
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

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 SPECIFICATIONS

Unit Title
Incident Response, Investigations and Forensics

Level
4

Learning Time Hours
200

Credit Value
20

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

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

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

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 SPECIFICATIONS

Unit Title
Security Strategy: Laws, Policies and Implementation

Level
4

Learning Time Hours
200

Credit Value
20

Unit aim
Knowing how to build a cyber defence strategy, what legal tools require consideration, how policies can be written and embedded, are all vital ingredients to successful in-house cyber security practices. In this unit the learner will bring together knowledge acquired from previous units and build on this in relation to developing plausible strategic plans, executive buy-in and legal compliance. Key questions and challenges are posed:
• What is 'strategy' and what can a 'cyber security strategy' look like?
• How do we achieve senior-level buy-in?
• How do we monitor and safeguard compliance, particularly if our operations are dispersed across a multinational environment?
• What are the key legal requirements and industry standards that can assist and enhance our cyber security strategies and practices?

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

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

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 SPECIFICATIONS

Unit Title
Cyber Security Threats and Risks: Banking and Finance

Level
4

Learning Time Hours
200

Credit Value

20

Unit aim

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

Learning outcomes and assessment criteria

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

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

Suggested Resources

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

UNIT SPECIFICATIONS

Unit Title

Cyber Wars

Level

4

Learning Time Hours

200

Credit Value

20

Unit 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 wide scale disruption and long-term power outage.

Learning outcomes and assessment criteria

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

Learning Outcome	Assessment Criteria
1. Understand how 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

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/innews/news/increasing-effect-geopolitics-cybersecurity

UNIT SPECIFICATIONS

Unit Title
Cryptography

Level
5

Learning Time Hours
300

Credit Value
30

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

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

Learning Outcome	Assessment Criteria
1. Understand key cryptographic principles and modes	1.1 Define the concept and application of cryptography 1.2 Explain symmetric and asymmetric modes and approaches 1.3 Assess how cryptographic methods and standards underpin the communications

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

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-ComputersSpies/dp/0297871730
- Krebs on Security (Online) accessed at: https://krebsonsecurity.com/
- Lawrence Miller and Peter Gregory (2018) CISSP For Dummies (USA: John Wiley & Sons), available at: https://www.amazon.co.uk/CISSP-Dummies-Computers-Lawrence-Miller/dp/0470537914

UNIT SPECIFICATIONS

Unit Title
Digital Investigations and Forensics

Level
5

Learning Time Hours
300

Credit Value
30

Unit aim
This unit describes and explains how to conduct investigations with cyber-enabled equipment, including on public-internet-facing networks, or other network environments. Much evidence is lost or ruled inadmissible within courts and tribunal environments because it has been mishandled and corrupted (or could have been) by investigators, or those with a perceived chain of custody over the data. Moreover, in a planet of several billion cyber-enabled devices, but few qualified cyber investigators, it is now the case that many organisations have to manage part or all of a cyber incident investigation, because the national CERT or police/security agencies are otherwise prioritised. In this unit learners will examine the requirements for digital investigations including team formations and tools, understanding the prospects of recovering information, gathering evidential data (including from mobile and IoT devices), safeguarding evidential integrity, as well as the complexity and challenges of storing and presenting evidence within legal environments. Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

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

Learning Outcome	Assessment Criteria
1. Understand the core principles of digital investigations	1.1 Explain the investigation lifecycle from initiation to conclusion 1.2 Explain how a 'digital' domain investigation is organised and managed
2. Apply the types of tool that support professional digital investigations at a strategic level	2.1 Analyse the range of tools that assist digital investigations in different situations 2.2 Select the appropriate tools to carry out a digital investigation for a given situation, justifying the selection
3. Plan for an investigations and forensics teams	3.1 Explain the types of skills required to undertake a variety of investigations and forensic-related work 3.2 Explain dynamics of forming and integrating digital investigation teams and

	geographically distributed and dispersed investigations and teams 3.3 Develop a plan for the formation of an investigation and forensics teams
4. Understand the importance of safeguarding evidential integrity in digital investigations	4.1 Explain how evidence can be retrieved from mobile devices and IoT devices 4.2 Analyse how evidential integrity is safeguarded during digital investigations 4.3 Assess how evidence is stored and presented within legal environments

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 SPECIFICATIONS

Unit Title
Communications and Incident Management

Level
5

Learning Time Hours
300

Credit Value
30

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

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

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

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-managementfor-cybersecurity-incident-response/

UNIT SPECIFICATIONS

Unit Title
Strategic Leadership

Level
5

Learning Time Hours
300

Credit Value
30

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

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

Learning Outcome	Assessment Criteria
1. Understand the role senior leaders and strategic leadership	1.1 Explain the key roles and responsibilities of senior leaders in a tech sector setting 1.2 Assess how strategic leadership and core goal-setting can enable stronger security cultures
2. Evaluate the management streams and performance monitoring mechanisms that relate to information security	2.1 Explain the importance of integrating management and operational programmes in relation to optimum levels of performance and cyber resilience 2.2 Anlayse the performance monitoring mechanisms in place to protect information security 2.3 Assess how cultural and diversity-related complexities impact on management and performance monitoring
3. Understand how threat and risk identification and management is integrated into C-Suite considerations and governance	3.1 Evaluate risk management and threat identification within the context of wider corporate strategy, responsibilities and governance 3.2 Explain the impact of poor or ineffective C-Suite understanding and direction 3.3 Assess the importance of business ethics and leadership in business values, including within end-user environments of ICT systems
4 Understand how data protection legislation impacts considerations of strategy-setting and strategic leadership	4.1 Evaluate how major data protection laws, impact on C Suite strategic level decision making and strategy setting 4.2 Assess the consequences for individuals and organisations of non-compliance with this legislation

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)

Version:2308a