H9BRIM: Business Resilience and Incident Management

Module Code:	H9BRIM
Long Title	Business Resilience and Incident Management APPROVED
Title	Business Resilience and Incident Management
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Vanessa Ayala-Rivera
Module Author:	Andrea Del Campo Dugova
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Evaluate incident response plans, their effectiveness and their alignment to industry leading standards and appropriate incident response principles and methodologies.
LO2	Critically appraise response activities for incident management from initial compromise to recovery and make recommendations for improvement.
LO3	Contrast methods to assess the maturity of an organisation's incident response capabilities.
LO4	Evaluate mechanisms to leverage blue team and the red team capabilities during an incident, and appraise appropriateness and prioritisation for specific incident response use cases.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9BRIM: Business Resilience and Incident Management

Module Content & Assessment

Indicative Content
Introduction • A background on the industry leading best practices (Including NIST IR Fundamentals). • Understanding what risk means for an organisation and how an event ties into risk management processes. • Providing an overview of where IR impacts governance, risk and compliance.
Assessing Impact of Cyber Attacks • Understanding the threat landscape, recent incidents and developments in IR tools and processes. • Overview of business resilience with business continuity and the IR focus on availability, while managing disruption.
System Security concepts • How Blue teams evaluate and defend systems and environments. • Understanding blue team activities during an incident with a focus on Windows and Linux OS Security and Azure.
Scaling Incident Response • Shaping and improving your IR posture. Focus on Red teams and how they play the role of attackers by identifying security vulnerabilities and launching attacks within a controlled environment. • Understanding when and how to use a red team during an incident.
IR Roles and Responsibilities • A mapping of IR roles to activities • How to prioritise these when directing incident response activities.
System Forensics and tools • The role of Incident Response, Forensics and E-discovery and the intersection. • Focus on system forensics and tools from an IR perspective.
Incident Response Steps • IR activities and processes to gain Business input for IR • What is required beyond the organisation for IR (i.e., NCSC, DPC Gardai, Legal etc.)
Business Processes • The business perspective on regulation and operational resilience, • The importance of process and service mapping to systems
Threat Intelligence • Threat intelligence processes • Importance of SIEM from threat hunting to performance monitoring
Security operations for IR • Approaches, processes and roles within Sec Ops for monitoring, the three-tiered model for SOC. • Threat intelligence processes and tooling.
IR Improvement process • How to evaluate your organisation's posture for IR • IR Reporting • IR Measurement • IR Auditing • IR Testing
Summary Re-cap on core domains and takeaways

Assessment Breakdown	%
Coursework	100.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	CA 1	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	1,2,3
Non-Marked:	No		

Assessment Description:
For this assessment students will have to evaluate real-world incidents and critique the incident response process. The CA is based on course content covered up to the date of assessment. Critical appraisal and evaluation required.

Assessment Type:	CA 2	**% of total:**	60
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
Terminal assessment based on 5 varied themes covered during the course requiring critical evaluation and demonstration of conceptual learning based on scenarios, research and critical appraisal.

No End of Module Assessment

No Workplace Assessment

Reassessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Reassessment Description
The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.

H9BRIM: Business Resilience and Incident Management

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning Time	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Module Resources

Recommended Book Resources

Steve Anson. (2020), Applied Incident Response, 1ST ED. John Wiley & Sons, p.464, [ISBN: 978-1119560265].

Yuri Diogenes,Erdal Ozkaya. (2022), Cybersecurity–Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system., 3RD ED. Packt Publishing, p.0, [ISBN: 978-1803248776].

James Crask. Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301., 1st Ed. Kogan Page, [ISBN: 978-1789668155].

Supplementary Book Resources

Arun E Thomas. (2018), Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence, [ISBN: 978-1643169705].

Richard Bejtlich. (2013), The practice of network security monitoring: understanding incident detection and response., 1st Ed. No Starch Press, p.578, [ISBN: 978-1593275099].

Wilson Bautista. (2018), Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents, Packt Publishing, p.316, [ISBN: 978-1788625562].

This module does not have any article/paper resources

Other Resources

[Website], Verizon Breach Report,
https://www.verizon.com/business/resourc es/reports/dbir/

[Website], Sans Reading Room,
https://www.sans.org/reading-room/whitep apers; https://www.sans.org/reading-room/

[Website], Incident Handler's Handbook,
https://www.sans.org/white-papers/33901/

[Website], Security Onion Solutions,
https://github.com/Security-Onion-Soluti ons/securityonion

Discussion Note:	