Appendix 2: UIS CSIMP Quick Reference Determining Cyber Security Crisis Thresholds'

1. The following is a guide to help decide whether a cyber security issue is an incident or a crisis. The list is not an exhaustive list, it provides typical characteristics and aims to guide the decision.
2. Critical incidents are non-routine and there is often limited or inaccurate information about the cause of the incident.
3. Check each item on this list, tick as required and add up the scores. A score >7 is more likely to be a critical incident (crisis) than a standard incident; a score below <5 is more likely to be an incident, and best resolved with standard IT incident management processes.

Functional Impact - measure of the actual ongoing impact to the University (not only UIS)

	Tick if yes	Score if yes
• Service or system[1] critical to the operation of the University[2] suspected attack (or root cause not known)		+2
• Service or system critical to the operation of the University confirmed attack		+3
• Service or system critical to the day-to-day business of the University suspected attack (or root cause not known)		+1
• Service or system critical to the day-to-day business of the University confirmed attack		+2
• Standard service or system suspected or confirmed attack		+1
• Multiple independent services affected		+1

Privacy Impact: Number of individuals' data suspected or confirmed at risk

1 to 100 in a minor way		0
100 to 1000 in a minor way OR >= 1 severely		+1
1000 to 10000 in a minor way OR >= 10 severely		+2
10000+ in a minor way OR >= 100 severely		+3

Research Impact: the number of research groups or research studies suspected or confirmed at risk

1-10 in a minor way		0
10-100 in a minor way OR >= 1 severely		+1
>100 in a minor way OR >=10 severely		+2

Teaching impact: the number of students suspected or confirmed at risk

<=10 Undergraduate OR postgraduate groups in a minor way		0
>=10 Undergraduate and postgraduate groups severely		+1
Undergraduate exams OR postgraduate exams or thesis severely		+2

Reputation Impact

Local press, low exposure **OR** Internal matter		+0
Detected or reported in the public domain (including social media – but not mainstream)?		+1
National press, low exposure		+1
National adverse media attention		+2
Detected or reported by mainstream media? **OR** Continual adverse media attention attached to name		+3
Detected or reported by ICO / OfS / HMG?		+2
Detected or reported by a funding organisation / major donor?		+1

Recoverability Impact – scope of resources needed to recover from the incident

Can be handed by internal teams within the operational target with an effective plan for resolution		0
External Technical teams support is needed and no effective plan for resolution		+1

[1] As defined in the *IT Service Tiers* on the UIS intranet. System and Service can be interpreted interchangeably

[2] Operation of the University includes systems and services provided to students, employees, visitors.