



SDI Review Form 1.6

Journal Name:	British Journal of Mathematics & Computer Science
Manuscript Number:	2014_BJMCS_11874
Title of the Manuscript:	A Comparative Assessment of Computer Security Incidence Handling
Type of the Article	Review Article

General guideline for Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty**', provided the manuscript is scientifically robust and technically sound.

To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(<http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline>)



SDI Review Form 1.6

PART 1: Review Comments

	Reviewer's comment	Author's comment (if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)
Compulsory REVISION comments	1. The author should cite and introduce more recent and valuable state-of-the-art approaches about incident response. 2. The references are not up-to-date enough. Make sure that there are several references in recent three years, 2011-2014. A review article is better to investigate some up-to-date studies.	1. Recent (2012-13) literatures have been introduced. See lines 36-41, 207-250. 2. Incidence response approach is only considered when a majority consider it reasonably and generically applicable. So the manuscript has been updated accordingly with updated studies. Updates and reviews will continue as new approaches emerge.
Minor REVISION comments	1. In line 43, add "." at the end of the sentence. 2. In line 206, "[1], [2] and [4]" → "[1,2,4]". 3. In line 217, ";" → ":". 4. In line 221, 222, the sentence "These processes ... threats." → "These processes include preparation, detection, formulation of response strategy/planning, containment/preservation, eradication, recovery and lesson learned/reporting/follow-up and incident closure. All of these processes should be managed in a collaborative manner given the distributed nature of modern-day threats, which is shown in Fig. 1." 5. The caption of the figure should be added, such as "Fig. 1 ..." 6. In last sentence of <i>ii</i> in section III, ";" → ":". 7. The spacing between <i>ii</i> and <i>iii</i> in section III is too large. 8. The title of <i>iv</i>, "Containment / Preservation" → "Containment/Preservation".	1. Appropriate correction is effected. See line 2. The citation order used in the manuscript is the automated "IEEE-Reference Order", which is same as the manual style proposed by the reviewer. The automated style does not allow for the integration of authors within a single square bracket. 3. The ";" is more appropriate for introducing listings within a paragraph body. 4. Correction effected as proposed, see lines 273-274. 5. Caption added as suggested, see lines 278. 6. In last sentence of <i>ii</i> in section III, ";" comes more appropriate for furthering an already presented idea. See lines 289-290. 7. Correction effected appropriately, see line 291. 8. Corrected accordingly, see line 296 and 274
Optional/General comments	This review article introduces several related works of incident response such as Stepwise Forensic approach, Security Coordination Model, and so on. The analysis and discussions of unifying the approaches were clearly completed. It is a good work to understand the process of incident response and handling. However, the references are not up-to-date enough.	References updated accordingly as relevant.