**CyberSecurity Command Center Criteria for Sponsoring a Challenge**

**Objectives of CyberSecurity Command Center**

* Raise the level of cyber security awareness to our members/audience
* Educate the value proposition around healthcare privacy cyber security awareness and understanding
* Understanding the current and emerging threat landscape and challenges in the healthcare privacy and cyber security
* Showcase solutions on threats and challenges that the healthcare IT industry are facing today and tomorrow

**Challenges – requirements**

1. Must have accurate educational content.
	1. Must be vendor-neutral (vendor branding of challenge is okay, but challenge must contain substantive educational content).
2. Must have present/up to date content (not contain content which is outdated or outmoded).
3. Must be interactive with the attendee.
	1. Must provide visual information or audio information to attendee, or a combination of both.
		1. If audio is provided (or audiovisual), must provide headphones for attendees.
	2. Must provide the attendee feedback on how he or she is doing in terms of learning the educational content.
	3. Must tell the attendee what their strengths as well as weaknesses are re: educational content.
4. Must tackle a challenge in healthcare information security.
5. Must showcase our healthcare industry positively (not negatively) in all respects.
6. Must be respectful and encouraging in terms of the educational content, materials, and feedback to attendees.
7. Must link to or reference at least two (2) [HIMSS privacy and security resources](http://www.himss.org/library/healthcare-privacy-security) for attendees that want to learn more about educational content.
	1. May contain specific links to HIMSS Toolkit resources.
8. Must reference speaking session.
9. Must reference booth materials (in turnkey kiosk).
10. If there are multiple modules, the aggregate time must not exceed 10 minutes.
	1. Recommended time per module: 2-3 minutes.
11. Must supply contact information for more questions, etc.
12. At the end of the challenge, it is ok to refer to relevant products/services relevant to the challenge at the end and, as applicable, exhibit booth #(s) tied to products/services mentioned.

**Proposals – requirements**

1. Proposal must list at least 1 Cybersecurity Command Center booth objective which it satisfies (listed above).
2. Proposal must state who the stakeholders are that would be interested in the challenge and in what type of organization(s).
3. Proposal must state the educational level of the content.
	1. Beginner
	2. Advanced
	3. Intermediate
4. Proposal must meet the challenge requirements listed above.

**If questions, please contact you HIMSS Sales Representative**