Dear Conference Organizers,

I am have been developing a thesis regarding what I call the norm for individual security of property, particularly as it relates to questions of cyber security and information technologies. I have a working draft of a paper on this topic and would like to submit the slightly extended abstract below for consideration for the upcoming conference on March 29th, 2016, in Las Vegas. My paper could plausibly be considered for either the Security Conference or the Ethics Conference. I have a full-length working paper I could present, or I could present a more informal discussion of the issue. This work is being done as part of my research for a National Science Foundation Grant I was awarded to investigate the ethics and policy implications of cyberwarfare and cyber security. Thank you for your consideration.

Name: Bradley J. Strawser

Affiliation: Assistant Professor of Philosophy, Defense Analysis Department, US Naval Postgraduate School.

Website: www.bradleystrawser.com

Title: "Ethical Responsibility for Cyber Security: Changing Norms"

Abstract:

Recent high-profile hacking incidents caused critics on social media to blame the celebrities who were hacked rather than the hackers. They claimed that those whose risqué photos were stolen were to blame for failing to secure them. While such attempts to blameshift can be dismissed as victim-blaming, they elucidate a set of questions about the ethics of personal responsibility as it relates to computer security. Is the normative standard for security in the cyber realm in any way significantly different than the moral norms governing all other aspects of life with respect to questions of individual responsibility, blame, and negligence? For example, if I lock my possessions in my home, I have a reasonable expectation that they are safe from theft. But even if my house is unlocked with my possessions visible, few would argue that I deserve to be robbed due to my failure to secure my valuables. It would be an implausible stretch to assert that my negligence constituted a lack of blameworthiness on behalf of the thieves, or provided any mitigation to the moral wrongness of the act of robbery. Consider another more poignant example for the cyber-world. Imagine a man walking through a neighborhood checking doors to see if they are unlocked, but not stealing anything. Few would consider such behavior acceptable within present societal norms. Yet, in the cyber world, such norms have significantly less traction. Such thinking raises two important questions. First, does

the average person have the wherewithal to implement adequate or effective computer security? Second, whatever the cyber-equivalent to the norm of traditional security is, is there a prevailing belief that failing to meet it is a matter of negligence in the cyber case where the equivalent failing would not be considered negligent in the non-cyber case? Or, in other words, if a computer user's data is compromised did she, in some sense, "get what she deserved"? These questions have significant ethical and practical implications for cyber security and the various ways we interact with information and communication technologies on a daily basis.