

**Self-Assessment Survey:  
Does Layered Security Make Sense for Your Security Application?**

Roger G. Johnston, Ph.D., CPP  
Vulnerability Assessment Team  
Argonne National Laboratory

The following self-assessment can be used to determine if a new security layer makes sense (or if an existing layer should be maintained alongside other security layers). This self-assessment shouldn't be taken overly seriously—its not all that rigorous and the scoring is somewhat arbitrary—but it can nevertheless be useful for encouraging careful thinking about the layer in question.

Directions: Examine each of the 21 questions below about the security layer (or measure) of interest. For each question, decide if the answer is yes, no, or maybe/unknown. Circle your answer for each question. Scoring: Add up the number of circled answers in column B which we call NB. Add up the number of circled items in column D which we call ND. Your total score is  $(2 \cdot \text{NB}) + \text{ND}$ . (Column B contains the "ideal" answers if the security layer in question makes sense to implement or keep.)

Interpreting the score: The maximum possible score is 42. If the score is greater than 36, the security layer in question is probably a good idea. If the score is less than 29, the security layer is probably not a good idea and will likely decrease overall security. If the score is between 29 and 36 (inclusive), the security layer needs more analysis or modifications in terms of its effectiveness and interactions *vis a viz* the other security layers; thinking carefully about the questions in the table might help clarify the issues. Thus:

Score 37 to 42, the security layer in question is probably a good idea.

Score 29 to 36, the security layer needs more study, analysis, or refinement.

Score 0 to 28, the security layer is probably not a good idea and will likely decrease overall security.

Question	A	B	C	D
1. Is introduction of the new layer being used (consciously or unconsciously) to avoid having to think carefully about existing security vulnerabilities or how to optimize the existing layers?	yes	no		maybe/unknown
2. Is the new layer being installed out of fear or desperation or urgency or cognitive dissonance (mental tension between our hopes and our fears)?	yes	no		maybe/unknown
3. Is the new layer being installed primarily because funds become available for it, or because non-security managers or executives ordered it?	yes	no		maybe/unknown
4. Is the motivation for the new security layer essentially a “vitamin mentality”—“if some security is good, then more must be better”?	yes	no		maybe/unknown
5. Do you think the new layer is undefeatable?	yes	no		maybe/unknown
6. Have you taken steps to insure that alarms generated from the other security layers won't be ignored or discounted because of the existence of the new layer?		yes	no	maybe/unknown
7. Will the new layer distract security personnel or cause less attention to be paid to the other layers of security?	yes	no		maybe/unknown
8. Does the new layer have buy-in from the security personnel or others who must use it?		yes	no	maybe/unknown
9. Will the new layer dramatically increase the complexity of providing security, or the time and/or costs involved?	yes	no		maybe/unknown
10. Will installation of the new layer and the learning curve associated with it introduce an extended period of weakened security?	yes	no		maybe/unknown
11. Is the new layer <u>specifically</u> designed to deal with known vulnerabilities or attack modes for the other layers of security?		yes	no	maybe/unknown
12. Are there specific, rigorous reasons to believe the new layer will improve <u>your</u> security (as opposed to just relying on hope, speculation, sales hype, hearsay, or assumptions)?		yes	no	maybe/unknown
13. Can you summarize in 2-3 sentences (without relying on sales hype) exactly how the new layer will improve <u>your</u> security?		yes	no	maybe/unknown
14. Are the vulnerabilities and attack modes for the other layers of security well understood by you, and have you tried to defeat them?		yes	no	maybe/unknown
15. Are the vulnerabilities (including any software vulnerabilities) and attack modes for the new security layer well understood by you?		yes	no	maybe/unknown
16. Do you have a good understanding of how the new security layer works?		yes	no	maybe/unknown
17. Is the new layer of security relatively untested, and is it high-tech and generating a lot of buzz/hype/excitement?	yes	no		maybe/unknown
18. Are you clear on whether the new layer is meant to be serial, parallel, redundant (backup), or some combination?		yes	no	maybe/unknown
19. Are the skills and methods an adversary would use to attack the new layer similar to the other layer(s)?	yes	no		maybe/unknown
20. Are there serious common modes of failure, e.g., can one event neutralize multiple layers of security? (For example, if the electrical power is shut off by an adversary, will the new layer and other layer(s) stop working?)	yes	no		maybe/unknown
21. Does the new layer compete or interfere with existing security layers in terms of physical space (e.g., there isn't enough room in the hasp for both a lock and a seal), maintenance, upgrades, funding, attention by frontline personnel, power requirements, or electrical/radio frequency interference?	yes	no		maybe/unknown

<p>Instructions:</p> <ol style="list-style-type: none"> <li>1. Total up the number of items circled in column B = NB.</li> <li>2. Total up the number of items circled in column D = ND.</li> <li>3. Score = (2 * NB) + ND.</li> </ol>		NB =		ND =
Final Score = 2NB + ND =				