AuditLink
CU*ANSWERS Management Services

October 8, 2015

The Case for Voluntary Use of the FFIEC Cybersecurity Tool

Patrick Sickels, Internal Auditor

CU*Answers is of the opinion that the FFIEC Cybersecurity Assessment Tool should be voluntary for credit unions. CU*Answers agrees with CUNA's review that the Tool has value, but is likely to take far longer than the 80 hours estimated by the FFIEC, and there are significant problems with the Tool itself. Credit unions should review the Tool and determine whether or not there is value to the institution in completing this tool.

The Inherent Risk Profile Tool is fairly well written and there are some advantages to using the Profile for your own assessments. There are only 39 total categories, and all of them touch on some level cybersecurity issues that every financial institutions should be reviewing. If these subjects are applicable to the financial institution, its security policies and/or Information Security Program ought to consider and address them.

There are some issues with the Inherent Risk Profile Tool. For one, the category of risk for each individual category can seem rather arbitrary. For example, an institution jumps from "Minimal Risk" to "Moderate Risk" depending on whether it has 20 ISP connections or 21 ISP connections. On the wireless category, the assessment begins with concern about whether there is Guest Access or not, but this concern is dropped if the credit union has over 250 users and 26+ access points. In addition, each category is weighted equally, when the actual risk to the institution is much greater. For example, a financial institution that allows fax and phone wire transfer risks is considered to be at "Moderate Risk" if the daily wire volume is at 3-5% of total assets; while if the institution has over 200 ISP connections it is considered to be at "Most Risk." In reality, the institution that only does in-person wire transfers is probably at much less risk than having numerous ISP connections from its branches, but the Tool does not weigh these answers differently. Finally, the Inherent Risk Profile Tool does not consider any compensating controls whatsoever in developing a risk score.

Despite its problems, the Inherent Risk Profile Tool does a decent enough job of estimating an institution's cybersecurity risk and it may make sense for a credit union to go through this exercise, especially if it has not conducted a regular annual cybersecurity review.

The same positives cannot be said about the Cybersecurity Maturity Tool. Per the FFIEC, credit union management is supposed to look at its inherent risk as mapped by the Tool, and then determine the organization's "maturity" by answering a list of questions. In theory, a credit union should do a gap analysis to see whether its maturity is lower than its inherent risk profile suggests.

There are significant problems with this approach. First of all, the Maturity Model statements are not well correlated to the risks identified in the FFIEC Inherent Risk Tool. Second, there is a significant amount of arbitrariness in the ranking of the various Maturity levels. (The FFIEC requires that a financial institution meet all of the categories of one Maturity before moving on to the next level). For example, to get to the "Advanced" Maturity of Oversight, an institution must be able to answer affirmatively that "The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy." This requirement is not well thought out and does not seem to have a clear relationship to cybersecurity. Clarity of expected output is missing in many of the Maturity Tool statements.

In addition, there are certain categories that do not appear at all to be relevant in the credit union space. Very few credit unions will be able to answer that "Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components." How would most credit unions accomplish this? Frankly, how would most international banks? It would seem more effective to be able to say that there will be alternatives available if there is an issue with the mission-critical equipment supplier. Finally, there is always the chance that a financial institution will get a negative connotation of being "immature" even if the credit union is well protected against cybersecurity threats for the size and risk profile of the institution. FSIAC has also weighed in and has launched an even more detailed critique of the Assessment Tools.

The only real positive in the Maturity Models is that the "baseline" models provide a financial institution with the basic compliance requirements it needs to meet with respect to cybersecurity. All credit union should review the "baseline" elements of the Cybersecurity Maturity to ensure compliance with FFIEC standards.

The FFIEC itself has declared that the use of its Tools is voluntary. The Tool is well-intentioned and does have some valuable assistance for credit unions launching their own cybersecurity programs. CU*Answers and AuditLink will be committing additional resources to assist credit unions in the coming months to meet the cybersecurity challenge and do well by protecting the information and assets of their membership.

*Patrick Sickels began his career as an attorney, and quickly branched out into the technological services industry, where he used his legal skills to help companies manage their compliance requirements. Patrick used these skills to develop into a classically trained auditor and risk manager. At CU*Answers, Patrick's background of law and technology make him uniquely suited to assist credit union clients in managing their risk requirements with a minimum of cost.*

Patrick is a licensed Certification Information Systems Auditor (CISA), as well as having the Risk and Information Systems Control (CRISC) designation. Patrick has done extensive work in designing risk models and control frameworks for a vast array of commercial, manufacturing, and financial firms. Patrick's specialty is the design of compliance models which meet legal standards at the lowest possible cost for the organization.