FINAL EXAMINATION

CYBE 5740 – Secure Acquisition

Name _____

Questions: (for 3 points each) - return to:

1. *Explain how the three communities of practice function in a multi-tiered supply chain structure? Why are suppliers likely to fulfill all three roles? What is the consequence of their doing that?*

Information technology SCRM is carried out across three risk management tiers or communities of practice. They are organization which includes leadership such as the CEO and CIO. An organizations mission which is carried out by mid-level management such as program managers, engineering oversight in SDLC, and acquisitions. At the base of this three-tiered pyramid is the information systems themselves. This area includes systems management, developers, system owners, and contracting personnel. Suppliers perform all three duties because they are independent entities with separate leadership and mission business goals that have their own multireed supply chain structure. As these suppliers are daisy chained together by the integrator and acquirer communication and oversight is essential because of operational complexity. It is important to have strong inter and intra tier communication that integrates strategic and tactical activities among all interested parties up and down the supply chain. This helps inform supply chain risk management activities as much as possible thereby reducing risk and increasing control.

2. *Why is it necessary to perform a functional decomposition of the product tree? Specifically, what does this allow you to control. Where does intangibility fit into this problem and how can it be addressed?*

One of the greatest challenges with implementing risk management frameworks and the controls that go along with them to information technology systems is intangibility. For example, a F-150 pickup truck fresh off the factory floor can be easily inventoried and the suppliers of the parts that went into the truck visually and physically categorized. With IT and software systems with multiple layers of abstraction going into software interfaces it can be very challenging to figure out who supplied which product. A functional decomposition of the product tree breaks this down like taking apart piece by piece a F-150 pickup. Each software module is broken down into its functional component and assigned to a supplier. This allows the integrator and acquirer to have situational awareness of their software supply chain down to the fundamental component. If a defect, security patch, or recall is identified it is very important for an entity to quickly identify the root supplier and begin steps to mitigate the issue.

3. *What is the justification for a well-defined SCRM process? And how do the communities of practice fit into the operation? More importantly, explain why the product tree is so important to establishing the assurance.*

A well defined SCRM process provides the framework to increase levels of quality, security, and reliability across a product line. A properly decomposed product tree

gives situational awareness across the communities of practice. Situational awareness that can be used by all three levels to ensure inter tier and intra tier communication up and down the organization. Effective communication from tier 3 (information systems) flows up through tier 2 (mission business processes) to tier 1 (organization) and provides a feedback loop to leadership to provide traceability and transparent supply chain risk decisions. The process is reversed from tier 3 to tier 1 to implement tactical level adjustments based on the information from the feedback loop. A properly decomposed product tree ensures that there are no oversights in situational awareness across the three communities of practice. Having oversights are gaps that create blind spots that malicious actors rely on to make a living.

4. *Explain the linkage between the specification and the contracting phases in the assurance of trusted products. Why are these two phases critically linked to the acceptance phase?*

Proposed software specifications are derived from a large set of agreed upon assumptions. Agreed upon assumptions for the operating environment, security requirements, and reliability to name a few. These specifications are then formalized into a request for proposal (RFP) that specifically states exactly what is needed to fulfill the requirements for a given software product deliverable. The RFP includes the statement of software functional requirements, statement of work, statement of objectives, work statement, and performance-based work statement. The RFP provides the legally binding contractual framework that the acceptance

phase relies on. The acceptance phase is where the acquirer takes custody of a given software product from the supplier. The acceptance phase is adversarial in nature as the acquirer is verifying the supplier delivered exactly what the RFP requires. A weak or incomplete RFP (contract) risks a weak or incomplete product as the supplier is not contractually obligated to deliver anything more or less than what the RFP requires.

5. *What is the role of the "Need to Acquire" document in the assurance of a secure product? Specifically, how does initial planning for product implementation impact the selection of options for product acquisition?*

The "Need to Acquire" document servers as the memorandum of understanding that defines contractually what will later become the formal request for proposal. The needs document could be the result of business planning and analysis or simply the impulse of a senior executive. The needs document usually starts within the business side of the entity and serves as a roadmap to locate accountabilities and conduct of the overall acquisition. It also provides the value statement for the given solution they are seeking to develop. Having a detailed problem/solution statement at the beginning of the project, clearly stated in the needs document helps ensure that the security requirements of the process are followed. The needs document also takes a look at how the new software solution will fit into existing systems. This ensures that integration issues are planned for and mitigated to the highest degree possible. Just like all software development endeavors getting as much of the planning done at the beginning reduces the cost of secure, quality software design.

6. *What is the role of capability maturity in the development and evaluation of a secure product? Which of the five types of SCRM failure outlined by the OMB does the concept of capability maturity directly address.*

NIST SP-800-161 states that ICT supply chain risk management builds on existing standardized practices in multiple disciplines. Essentially for an organization to be able to incorporate effective SCRM they must have reached a certain level of process maturity across a diverse set of internal operations. A maturity checklist like the ones we used for suppliers and acquirers does a capability gap analysis of a given organization to determine the level of maturity for each critical area. Implementing a SCRM process can be costly and time consuming and it is important to the mission of the organization that SCRM does not act as a sea anchor to accomplishing their given mission. OMB A-130 Responsibilities for Protecting and Managing Federal Information Resources outlines five major threats. They are environmental disruptions, purposeful attacks, structural failures, human errors, and new/emerging. A maturity checklist helps address the human error element in the supply chain.

7. *What is the role of explicitly designed and monitored controls in the assurance of sourced products, or services? How can a formal standard be used to create an effective control structure?*

Once a supply chain's product has been decomposed and each entity within it explicitly linked to a deliverable a control framework can be implemented to increase security and quality. The entities within a supply chain generally fall under

one of three categories, acquirer, integrator, and service provider. These entities each have a different framework for SCRM maturity and different regulatory requirements especially under U.S. Federal ICT product delivery. If operating under the U.S. Federal system these entities will use the NIST frameworks such SP 800-53 Rev 4 for base IT security controls and overlay that with SP 800-161 for SCRM specific controls that compliment and map to their parent framework in 800-53 rev 4. In pursuit of defense at depth across a multi-tiered system this structure provides continuous layers that reduces gaps in security practice as much as possible. Using a best practice framework increases effectiveness, reproducibility, and standardization across large enterprises and communities of practice. All of which are good for security.

8. *What is a mitigation? What is the role of identification and risk analysis in developing effective mitigations for the supply chain? Is this a dynamic process (meaning can it change in-stream)? If it is how are mitigations maintained?*

A mitigation is a control applied to the explicit identification and quantification of a given threat, threat actor, or attack vector to a specific organization's operations. To mitigate a given threat an entity may accept the risk with control or controls to reduce the likely hood and impact or transfer the risk to another entity. The challenge with supply chain risk management is the opaqueness of supplier networks as they move further down a given product line. This opaqueness reduces product quality and security situational awareness and increases complexity. Both

of which are things that increase the likelihood of a quality or security event occurring. Comprehensive product supply decomposition along with risk analysis of this decomposed product line increase the visibility into the supply chain. Risk analysis is a dynamic process compromising framing risk, assessing risk, responding to risk, and monitoring risk. This process never stops it iterates over and over again just like the threats to a given entities IT system constantly evolve. Mitigations are maintained by evaluating their effective at reducing or transferring the specific risk being faced. New mitigations can be added and old less effective mitigations can be removed to save resources. This is done through a continuous testing and validation regime of the mitigations being used.

9. *What is the role of measurement and metrics in the overall Acquisition/SCRM process? What does measurement allow an organization to do that might be extremely attractive for businesses?*

Measurement and metrics allow any organization to make data driven decisions. Data driven decisions are important in finding hidden truth within an organization's operations. This allows an entity to make well informed security decisions that are void of any personal bias, blind spots, or emotion. In acquisition/SCRM an organization could build a data driven dashboard platform to track key metrics within the maturity model. Once tracked this would help an entity rapidly increase the maturity scores across the board. Acquirers looking to find new suppliers could be easily sold on the performance of a given entity if they have strong analytic

methods to back up their claims of security and quality in their product being delivered.

10. *What is the difference between (internal) supplier and (external) acquirer audits in the Acquisition process? Provide a justification for using both approaches in effective, long term product/services assurance.*

Organizations external information systems include those of the system integrators, suppliers, and external service providers. Unlike in an acquirer's internal organization where direct and continuous monitoring is possible, in the external supplier relationship, information may be shared on an as needed basis. The required level and frequency of this sharing should be clearly written in an agreement. IT supply chain infrastructure from external IT systems should be audited to ensure compliance to quality and security standards. Trust but verify is one of the best due diligence business philosophies to live by. Making sure that your supplier network understands up front the level of oversight they can expect to receive and then codifying that into whatever contractual framework that is used is critical to ensure no surprises are encountered in a long-term product/service relationship.