Joshua Main-Smith
November 1, 2020

Risk Assessment

1. **(10 points) As part of a formal risk assessment of the main file server for a small legal firm, you have identified the asset "integrity of the accounting records on the server" and the threat "financial fraud by an employee, disguised by altering the accounting records." Suggest reasonable values for the items in the risk register for this asset and threat with justifications for your choice.**

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Server accounting record integrity	Altered accounting records by employee – financial fraud	None	Unlikely	Catastrophic	Extreme	1

Since there was no mention of control measures, I will assume there is none. I chose the likelihood to be unlikely because, according to the 2020 Data Breach Investigations Report, the attack source was most likely external with the likelihood of it being internal is not insignificant, but less likely. As for the consequence, I was leaning between major and catastrophic. The latter seemed more fitting when taking into consideration that this is a *small* legal firm. Smaller businesses are at greater risk of failure, especially within the first couple of years of opening. Depending on the financial health of the legal firm along with the duration and significance of the fraud the consequence could be anywhere from moderate to catastrophic. The level of risk was determined given the relationship between the likelihood and consequence of the threat. This relationship can be seen from the table given below (taken from the Risk Assessment lecture). With this being the only asset listed, and risk priority of 1 was assigned.

2. **(10 points) Consider the risk to "integrity of the accounting records on the server" from "financial fraud by an employee, disguised by altering the accounting records," as discussed in Problem 1. From the list in NIST 800-53, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.**

The most fitting control would be the Audit and Accountability control family (AU ID in Table 1 from NIST 800-53 or under the Technical class from Table 15.1 from the textbook). Specifically, AU-3 Content of Audit Records and AU-6 Audit Review, Analysis, and Reporting (Appendix F from NIST 800-53). AU-3 allows for records to be kept for what events that occur, when an event occurs, where an event occurred, source of the event, outcome, and individuals associated with the event. AU-6 allows an organization (removing any individuals that have a conflict of interest) to review any anomalies in the reports generated from the events described above. Any anomalies are then reported to proper personnel. The effort here to generate such reports are low and provides a security measure that discourages fraudulent behavior and a

means to report, audit and review any anomalous behavior.

3. **(10 points) As part of a formal risk assessment of the external server in a small Web design company, you have identified the asset "integrity of the organization's Web server" and the threat "hacking and defacement of the Web server." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.**

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Web server integrity	Hacking & defacement of web server	None	Possible	Moderate	High	1

If an organization is under attack, then the nature of it will most likely be an attack on web applications or etc. This will make a web design company an enticing target for attackers and is the reason this will be more likely than the scenario given in problem 1. What makes the likelihood of this categorized as possible rather than likely is because information organizations update their systems much quicker than the average industry, discouraging those who are less experienced from attempting an attack. The consequence of hacking or defacement of the web server depends on the contents of the server and its function in the continued operation of the industry. I selected moderate sort of as a middle answer, but if the web server is hosting the main content of the organization then the consequence would be higher. Alternatively, if the web server contains a backup of their current hosting system (redundancy), then the issue would be less serious (although would put the company at risk if not fixed in a timely manner). The level of risk was determined using the table from lecture (see below) and the risk priority was selected due to this being the only asset listed.

4. **(10 points) Consider the risk to "integrity of the organization's Web server" from "hacking and defacement of the Web server," as discussed in Problem 3. From the list in NIST 800-53, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective.**

One thing to take into consideration is if an external connection to this web server is expected behavior or not, i.e. is this a server that only employees should have access to or is it public facing. If this web server is only for employee connections, then IA-3 Device Identification and Authentication may be a decent control option. This only allows devices that are uniquely identified to connect remotely, locally, etc. An attacker would need to know what unique identification is required for authentication. Further, even if an attacker acquires credentials to access a system (via phishing, for example) the attacker would still need to know the unique identification of the device to connect (to spoof their identification, for instance). If the organization has a large technical infrastructure, CA-8 Penetration Testing may be a good option to determine if an attacker is even able to reach the web server in question. If the organization has a small technical infrastructure, CA-8 may not be very cost effective. If the server is public

facing, then IA-8 Identification and Authentication (non-org) uniquely identifies non-organizational users by requiring user verification in some way before the user can use the system, such as 3rd party credentials. This would specifically apply to IA-8 (2).

5. **(20 points) Research the IT security policy used by your university or by some other organization you are associated with. Identify which of the topics listed in Section 14.2 this policy addresses. If possible, identify any legal or regulatory requirements that apply to the organization. Do you believe the policy appropriately addresses all relevant issues? Are there any topics the policy should address but does not?**

   The scope and purpose of the policy

   Yes

   The relationship of the security objectives to the organization's legal and regulatory obligations, and its business objectives

   Yes

   IT security requirements in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability, particularly with regard to the views of the asset owners

   Yes

   The assignment of responsibilities relating to the management of IT security and the organizational infrastructure

   Yes

   The risk management approach adopted by the organization

   Yes

   How security awareness and training is to be handled

   No

   General personnel issues, especially for those in positions of trust

   Yes, also this

   Any legal sanctions that may be imposed on staff, and the conditions under which such penalties apply

   No

   Integration of security into systems development and procurement

   Yes

   Definition of the information classification scheme used across the organization

   Yes

   Contingency and business continuity planning

   Yes

   Incident detection and handling processes

   Yes

   How and when this policy should be reviewed

   Yes

   The method for controlling changes to this policy

   Yes

   There were two topics that couldn't find on the UF IT policy page (https://it.ufl.edu/policies/). These were *How security awareness and training is to be handled* and *Any legal sanctions that*

may be imposed on staff, and the conditions under which such penalties apply. There were several pages indicating that staff or student would be trained under certain circumstances, but there was no mention of how this would be handled (at least from what I could find). I also couldn't find any policy that discussed the process in handling an employee under legal sanction. These relevant security policies should be discussed more or be more readily accessible. Some of the requirements that UF is legally liable to enforce or mitigate include copyright infringement, advertisement regulation, data loss or unauthorized disclosure, and violations of acceptable use policy.

Table Taken from Risk Assessment Lecture

	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	Extreme	Extreme	Extreme	Extreme	High	High
Likely	Extreme	Extreme	Extreme	High	High	Medium
Possible	Extreme	Extreme	Extreme	High	Medium	Low
Unlikely	Extreme	Extreme	High	Medium	Low	Low
Rare	Extreme	High	High	Medium	Low	Low