1. **If an organization has three information assets to evaluate for risk management, as shown in the accompanying data, which vulnerability should be evaluated for addi�tional controls first? Which one should be evaluated last?**

    First, I would calculate the risk of vulnerability by using the formula:
    Rr = (Lv x I)(1 – Rc + U)
    Switch L47 vulnerability 1 = (0.2 x 90)(1 – 0 + 0.25)
    = 22.5
    Switch L47 vulnerability 2 = (0.1 x 90)(1 – 0 + 0.25)
    = 11.25
    Server WebSrv6 vulnerability 3 = (0.1 x 100)(1 – 0.75 + 0.2)
    = 4.5
    MGMT45 control console vulnerability 4 = (0.1 x 5)(1 – 0 + 0.1)
    = 0.55

- Therefore, the vulnerability of Switch L47 would need to evaluated first because it has the highest risk rate (22.5) and the MGMT45 control console would be evaluated last because it has the lowest risk rate (0.55).

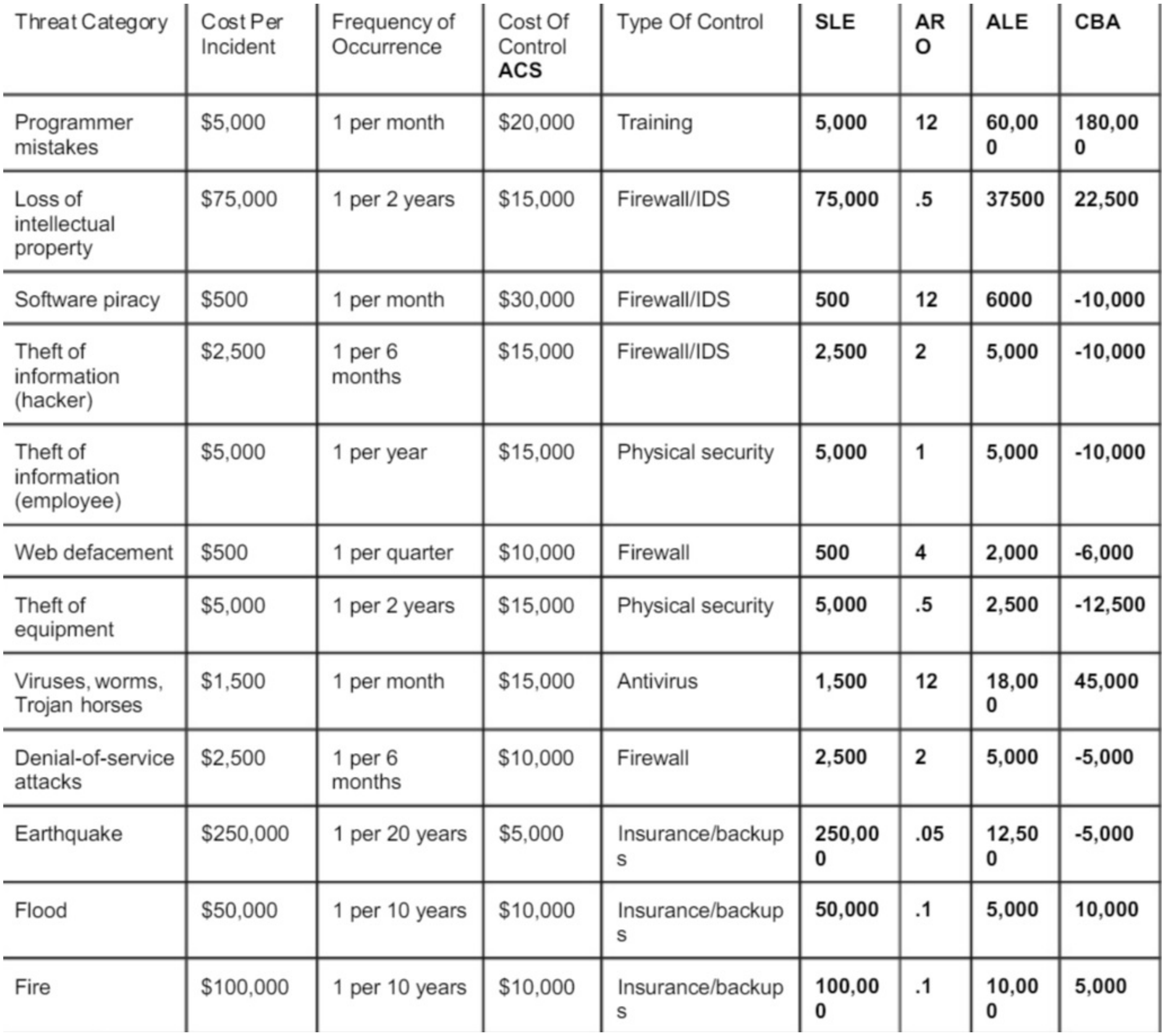
2. **Using the data classification scheme presented in this chapter, identify and classify the information contained in your personal computer or personal digital assistant. Based on the potential for misuse or embarrassment, what information would be confidential, sensitive but unclassified, or for public release?**

- My passwords, credit card information, social security number, and anything else I don't want others to see are examples of confidential information. Things I allow close friends or family members to see, such as usernames or banking documents, are examples of sensitive but unclassified (internal) information. Any information that I wouldn't mind others knowing would be considered for public distribution. Consider social media posts.

3. **Suppose XYZ Software Company has a new application development project, with projected revenues of $1,200,000. Using the following table, calculate the ARO and ALE for each threat category that XYZ Software Company faces for this**

project.

- ARO = Annualized Rate of Occurrence (expected frequency of an attack on a per-year basis). ALE = Annualized Loss Expectancy (calculated from ARO and SLE [single loss expectancy])



Threat Category	Cost Per Incident	Frequency of Occurrence	Cost Of Control **ACS**	Type Of Control	**SLE**	**ARO**	**ALE**	**CBA**
Programmer mistakes	$5,000	1 per month	$20,000	Training	**5,000**	**12**	**60,000**	**180,000**
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS	**75,000**	**.5**	**37500**	**22,500**
Software piracy	$500	1 per month	$30,000	Firewall/IDS	**500**	**12**	**6000**	**-10,000**
Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS	**2,500**	**2**	**5,000**	**-10,000**
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security	**5,000**	**1**	**5,000**	**-10,000**
Web defacement	$500	1 per quarter	$10,000	Firewall	**500**	**4**	**2,000**	**-6,000**
Theft of equipment	$5,000	1 per 2 years	$15,000	Physical security	**5,000**	**.5**	**2,500**	**-12,500**
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Antivirus	**1,500**	**12**	**18,000**	**45,000**
Denial-of-service attacks	$2,500	1 per 6 months	$10,000	Firewall	**2,500**	**2**	**5,000**	**-5,000**
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/backups	**250,000**	**.05**	**12,500**	**-5,000**
Flood	$50,000	1 per 10 years	$10,000	Insurance/backups	**50,000**	**.1**	**5,000**	**10,000**
Fire	$100,000	1 per 10 years	$10,000	Insurance/backups	**100,000**	**.1**	**10,000**	**5,000**