Risk Assessment : Maranyane lab

By: Roger Asquith

Overview of Risk Assessment

- What is risk assessment?
  - It is used to identify potential hazards and risk in a situation. It determines which measures that should be implemented to mitigate or resolve a risk.
- How it's measured
  - A risk matrix is used to figure out the potential risk of a situation. The likelihood and how severe the situation is measured on a 1 to 5 scale. It is then multiplied and analyzed.

Likelihood	Negligible	Minor	Moderate	Major	Disastrous
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Severity	1	2	3	4	5

Cybersecurity Risk in General

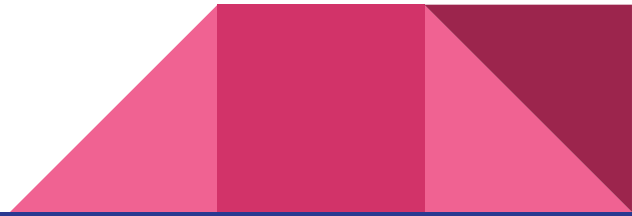
- The common types of cyber attacks for a laboratory are.
  - Opportunist attacks
  - Targeted attacks
- Common Risk
  - Software Access
  - Physical Access
  - Privileged Users
  - Social Engineering

Cyber Security risk at Maranyane lab

- The most common risk Maranyane has to face
  - Hacking, compromise, and unsure infrastructure
- Hacking
  - Malware
  - Phishing
  - Social Engineering
- Compromise
  - Network and endpoints
- Unsure infrastructure
  - Regarding to the laptops and they have electronics and the network its set up to.

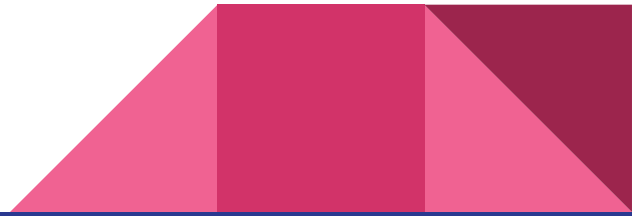
Hacking

- How does hacking work?
  - Social engineering
  - Hacking passwords
  - Infecting computers with malware
  - Logging keystrokes
- The effects of hacking at a laboratory.
  - Black mail
  - Theft of trade secrets
  - Down time issues



Hacking : Mitigation

- How to mitigate hacking.
  - Make sure software is up to date
  - Disable connects when not in use
  - Only use trusted applications
  - Review network and device names
  - Install MFA
- What to do after a hacker.
  - Notify people in charge
  - Change passwords associated with the account
  - Inspect devices.



Compromise

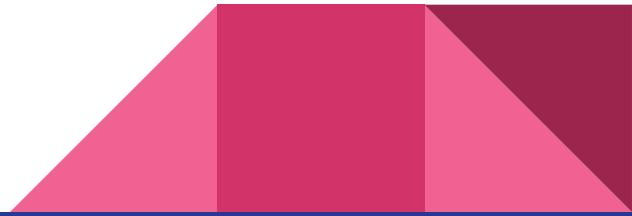
- What’s the risk?
  - Network,Endpoints, and Computers
- The effects when your Network is compromised
  - Frequent pop-up windows, especially the ones that encourage you to visit unusual sites, or download antivirus or other software
  - Changes to your home page
  - Mass emails being sent from your email account
  - Frequent crashes or unusually slow computer performance
  - Unknown programs that startup when you start your computer

Compromise : Mitigation

- What to do?
  - Reset passwords
  - Remove external hard drives
  - Scan for malware or virus
  - Monitor important financial or credit accounts
- How to prevent in the future
  - Practice password security
  - Backup files
  - Keep antivirus software up to date.

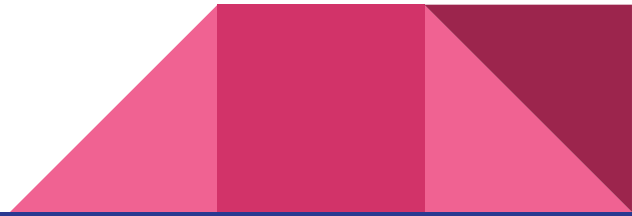
Infrastructure

- What is infrastructure.
  - When it relates to risk it involves identifying risk within the company and the technology and process used to minimize threats.
    - This can be applied by identifying all of the databases that have any personal information on them
- The effects when infrastructure is compromised.
  - Financial loss
  - Data loss
  - Company information leaked.



Infrastructure : Mitigation

- What to do?
  - Ensure that risk mitigation tools are strong
  - Double check and update software to stay ahead of bad actors
  - Add visibility for your cyber assets.



Original Risk Matrix

Likelihood	Negligible	Minor	Moderate	Major	Disastrous
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Severity	1	2	3	4	5

- Hacking
  - 10 (Disastrous)
- Infrastructure
  - 10 (Disastrous)
- Compromise
  - 10 (Disastrous)
- Likelihood
  - The likelihood for all focuses based on the fact there is no cybersecurity risk assessment in the first place and that the lab only has 3 employees.
- Severity
  - The severity is based on the effects of a security attack at the Maranyane lab.

Risk Matrix after Mitigation

Likelihood	Negligible	Minor	Moderate	Major	Disastrous
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Severity	1	2	3	4	5

- Hacking
  - 5 (Disastrous)
- Infrastructure
  - 5 (Disastrous)
- Compromise
  - 5 (Disastrous)
- Likelihood
  - The likelihood decreases to 1 based on the mitigation techniques stated before.
- Severity
  - The severity is based on the effects of a security attack at the Maranyane lab. It stays the same because the outcomes of an attack are still disastrous.

Sources

- https://safetyculture.com/topics/risk-assessment/
- https://www.uthsc.edu/its/cybersecurity/compromised-computers.php
- https://www.kaspersky.com/resource-center/definitions/what-is-hacking
- https://biosistemika.com/blog/cybersecurity-risks-in-your-laboratory/
- https://www.ag.state.mn.us/consumer/publications/HowtoProtectYourselfAgainstHackers.asp
- https://www.adserosecurity.com/services/infrastructure-risk-assessment/#:~:text=An%20Infrastructure%20Risk%20Assessment%20is,consumer%20personal%20information%2C%20an%20asset.