INCIDENT RESPONSE

(IR) Incident Response is the process an organization handles a data breach or cyber attack.

STEPS (1-7)

1. **Preparation** – Having clear communication on how you would respond to a attack. Making sure the employees have the appropriate training with tools to ensure they are able to handle an attack.
2. **Identification** – being able to spot whether or not an attack is underway. Knowing when the incident took place and how you can mitigate any damage that may have occurred.
3. **Containment** – Ounce you have found an attack, you have to keep it within a closed spectrum making sure you limit the attack from spreading any further.
4. **Eradication –** after the attack is contained, the goal is to get rid of threat and wipe it from the system.
5. **Recovery** – Ounce a threat has been removed the system is then reverted back to a state where the cyberattack was no longer present within the system.
6. **Lesson Learned** – After an attack has been made you must take a step back figuring out what was done for them to penetrate the system. Learning from that information the system can be improved to prevent an attack of that matter from happening again.
7. **Ongoing Improvement** – Keeping in touch with how cyber threats occur, you can test your system, and make sure it's up to date so you can address any weakness to prevent and ensure you're ready for future attacks.

Incident Policy – The steps that a company has in place that they undergo when presented with a cyber-attack. Being efficient and quick to stop/haul a cyber threat from spreading and wipe it from the system.

Incident Response Plan - a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident.

With a documentation, it helps when under pressure with remembering the proper steps on what to do when battling a cyber-attack. Showing you what you can do stopping an attack from spreading or catching it before they can penetrate your system.

Enumeration - a data gathering process wherein a cyber attacker extracts information about a network.

When someone has breached your system, they looked for anything they can to try and breach your system. Looking for certain IP addresses or User names for the computers in the company. Then using that to try and exploit any weak points within the network.

Tunneling - the process by which VPN packets reach their intended destination, which is typically a private network.

When sending anything to someone, as in sending a text or image to a recipient, that file will be encrypted so that it protects the content of what you are sending so that nobody can still it.

Privacy-Enhanced Mail (PEM) is a de facto file format for storing and sending cryptographic keys, certificates, and other data.

The PEM is used to keep your information secure. As in using google and other sites, you information will remain safe due to the PEM and SSL integration of those sites