The 11 security principal

1. Security versus convenience.
2. It is impossible to eliminate all risks.
3. Rules of risk calculation and mitigating controls.
4. Not all risks must be mitigated.
5. Security is not just keeping the bad guys out.
6. ROI doesn’t work for security.
7. Defense In Depth.
8. Least Privilege.
9. CIA triad.
10. Deterrents, prevention, detection.
11. Prevention fails

Security versus convenience.

- An example of the security convenience bell curve would be a company's "password change frequency" policy.
- At first, the company's policy requires users to change their passwords every six months.
- In an attempt to make the company even more secure, the policy is modified so that users must change their password every three months.
- However, after a few times of changing their passwords, users find it difficult to remember them and start writing them on sticky notes that are then stuck to their monitors or under their keyboards.
- This is obviously not a good place for confidential data and ultimately makes the business less secure.

It is impossible to eliminate all risks.

- First, let's start with an accurate definition of risk. risk is the "exposure to the chance of injury or loss" or "a hazard or dangerous chance.
- The confusion comes from the fact that many people think that for a given security issue, there is a "fix" that completely eliminates any risk from that issue.
- You must understand that it is, without a doubt, 100 percent impossible to eliminate all risk from any technology, system, or even situation.
- For every mitigating control there is a discrete level of risk.

Rules of risk calculation and mitigating controls

- To appropriately compare different risks, we need a consistent method for calculating risk.
- Although a multitude of different risk equations are available, the most basic equation is as follows:
- Risk = Consequence × Probability.

Not all risks must be mitigated

- Avoid Let’s imagine that the regulation only applies to companies doing business in Texas. If your company can prosper without doing business in Texas, then you’ve just avoided the risk.
- Transfer Maybe you can transfer the risk to a third party. If you could outsource the part of your business that’s covered by the regulation and let the third party worry about it, then you’d have transferred the risk.
- Mitigate If instead of avoiding, transferring, or accepting the risk, you might decide to implement controls to adhere to the regulation. Thus, you would have effectively mitigated the risk of a fine due to the regulation.

Security is not just keeping the bad guys out

- Security is not just about keeping the bad guys out.
- An extremely common misconception is that the primary concern for security administrators is keeping malicious outsiders from accessing critical systems.

ROI doesn’t work for security

- The traditional calculation of return on investment (ROI) doesn’t work for expenditures for security. At a very basic level, the calculation for return on investment determines how much profit will be produced if you invest X amount of money (or resources) into something.
- Using the ROI model, you can compare multiple investments and determine which is appropriate. Therefore, spending money on security cannot be justified with ROI, because it’s not a revenue-generating business process.
- You’re spending money (and resources) to protect a greater amount of money (or resources) from being lost.

Defense In Depth

- A defense-in-depth strategy, a security-in-depth strategy, refers to a cybersecurity approach that uses multiple layers of security for holistic protection.

Least Privilege

- You can improve security with Least Privilege. One of the most important and often overlooked methods for configuring security devices and implementing policies is that of Least Privilege.
- Least Privilege means giving users the bare minimum rights they need to perform their duties and then giving them additional privileges as necessary.
- The opposite way (the most common) is to give the most amount of privileges and then remove “dangerous” privileges one by one. This can also be referred to as blacklisting versus whitelisting

CIA triad

- Confidentiality Ensure that only those with the rights to view the data have access to do so, and prevent unauthorized disclosure of sensitive information.
- Integrity Ensure that changes made to the data are made only by authorized individuals, and prevent unauthorized modifications of systems and data.
- Availability Ensure that access to the data is available when needed, and prevent disruption of service and productivity

Prevention, Detection, Deterrents

- Prevention Aims to stop a certain activity before it happens.
- Examples:- include locks on doors, firewall.

- Detection Uncovers certain activities.
- Examples:-include motion-activated cameras and an intrusion detection system (IDS).

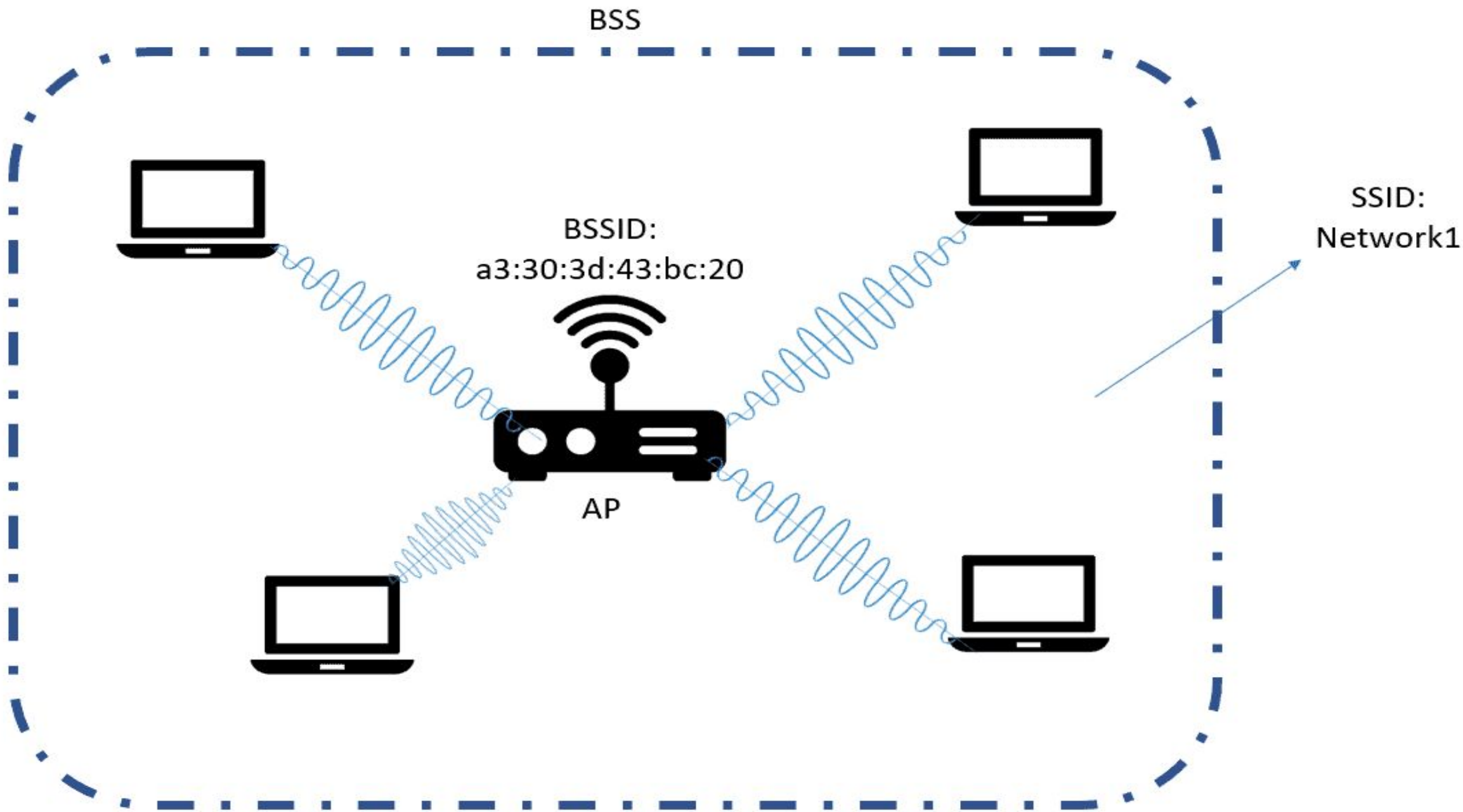
- Deterrents Security cameras can act as a logical deterrent because evidence of wrongdoing could be used in litigation against a perpetrator.

Prevention fails

- Any device can fail; make sure you perform maintenance and apply patches as needed to keep devices up to date and reduce the risk.

Access Points

- An access point is the device that allows multiple wireless devices to connect with each other.
- An access point connects multiple wireless devices together in a single wireless or multiple wireless networks.


BSS
BSSID:
a3:30:3d:43:bc:20
SSID:
Network1
AP

Types of access point

- Indoor (uses in home and offices)
- Outdoor(uses in factory or in industry or in outside of bungalows or in garden area)

Certifications for industrial grade access point

- IP 61 Protected from condensation.
- IP 62 Protected from water spray less than 15 degrees from vertical.
- IP 63 Protected from water spray less than 60 degrees from vertical.
- IP 64 Protected from water spray from any direction.
- IP 65 Protected from low pressure water jets from any direction.
- IP 66 Protected from high pressure water jets from any direction.
- IP 67 Protected from immersion between 15 centimeters and 1 meter in depth.
- IP 68 Protected from long term immersion up to a specified pressure.
- IP 69K Protected from steam-jet cleaning.

How AP Get Power

- POE – Power Over Ethernet
- POE Switch will generate the power and AP get power along with communication in single cable.
- If POE switch is not available access point can be power on using POE adapter.

Autonomous Access Points

- As the name autonomous implies, the controller allows the single device to manage traffic independently from any additional support.
- You can connect as many devices to it as you like (within the limits of the devices' design).
- If you need additional support for traffic, you can add autonomous access points and configure them to work together.
- This last part is why autonomous access points are not always the right answer.
- Manually configuring an autonomous workgroup can get prohibitively complicated. Those complications can make networks more expensive and less reliable.
- So, while autonomous points are amazing when working alone, when they need more help, they might not be the best option.

Controller Based Access Point

- Controller-based Access points are also known as thin clients and require a controller for centralized management.(updates, configuration, etc.)
- Controller based access points' for its centralized management, configuration, encryption, updates and policy settings through a centralized controller, they come with a cost.
- Do not need to be manually configured.
- Generally, Controller based Access points are generally used in large environments.

Architecture of wireless system

- WLC- Wireless LAN controller based

SSID

- SSID stands for Service Set Identifier.
- This is your network’s name.
- If you open the list of Wi-Fi networks on your laptop or phone, you’ll see a list of SSIDs.
- Wireless router or access points broadcast SSIDs so nearby devices can find and display any available networks.
- SSIDs can be up to 32 characters in length, but there are no restrictions for minimum size.

BSSID

- BSSID stands for Basic Service Set Identifier.
- It’s the MAC physical address of the access point or wireless router that is used to connect to the Wi-Fi.
- The BSSID is a 48-bit hexadecimal number.
- On the Windows OS, you can run the command netsh wlan show interfaces to find “BSSID”.

```
C:\Users\[redacted]>netsh wlan show interfaces

There is 1 interface on the system:

    Name                   : Wireless Network Connection
    Description            : Intel(R) Centrino(R) Advanced-N 6205
    GUID                   : 0be60353-ffee-4c24-95f4-66f2bfd327d7
    Physical address       : 84:3a:4b:50:40:60
    State                  : connected
    SSID                   : Meraki-Corp
    BSSID                  : 02:18:5a:91:11:c0
    Network type           : Infrastructure
    Radio type             : 802.11n
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 300
    Transmit rate (Mbps)   : 300
    Signal                 : 54%
    Profile                : Meraki-Corp

    Hosted network status  : Not started
```

MAC ADDRESS

- A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network.
- Primarily specified as a unique identifier during device manufacturing, the MAC address is often found on a device's network interface card (NIC).

Beacons:-

- Wi-Fi beacons are relatively short, regular transmissions from access points (APs) with a purpose to inform user devices (clients)about available Wi-Fi services and near-by access points.
- Clients use beacons to decide which AP with which to connect.

Association and Authentication :-

- Association and authentication are performed by clients when they want to join a wireless network.
- Associating to an access point means that your client and the access point have “agreed upon” which parameters to use to ensure proper communication.
- Authentication is a way of verifying that you are authorized to connect to the network. There are multiple methods of authentication, and authentication happens prior to association.