What is the Recovery Point Objective (RPO)?
The amount of time a company can be without its data. After this point, it cannot function. Acceptable downtime.

What is the Recovery Time Objective (RTO)?
The time you are back to an operational state. Ideally before the RPO.

What is the MTTR?
The mean time to repair an item

What is the MTBF?
The mean time between a number of failures. It measures reliability.

How does WPS work?
You just need to push a button; no need to insert anything

List the forms of wireless encryption, from weakest to strongest.
WEP (also known as legacy) is the weakest, followed by WPA, WPA2, WPA2 CCMP (AES) 128 bit, and finally WPA3 GCMP(AES) 256 bit.

Why could your wireless speed be slow?
You are too far away, or there is a large file downloading.

If you disable the SSID, can it still be discovered?
Yes, you can find it using a Wireless packet sniffer (also known as a wireless scanner or wireless analyzer).

How can you stop unauthorised access to a wireless network?
MAC filtering

What is a Rogue AP?
It is an unauthorized access point

What is an Evil Twin?
An access point made to look like a legitimate one

Which form of wireless has no authentication?

Open System Authentication. WiFi Enhanced Open.

You log in to an airport WiFi network, but can't access the internet. Why?
You are on a captive portal

What is a captive portal?
It controls access to a wireless network. You need to enter your email address, subscribe to a premium package, or accept an AUP.

How can you bypass security on a captive portal?
Spoof a MAC address

Which wireless antennas can work between two buildings?
YAGI or omnidirectional

What is TKIP used for?
For backwards compatibility (legacy)

What is wireless PSK?
It is the password to a wireless router

What is a guest WiFi network?
A network that is separate from the corporate network and can be used by visitors or employees at lunchtime

What is a wireless disassociation attack?
An attack that disconnects you from the wireless network

How can you find out if rogue machines are on your wireless network?
Enable MAC filtering and see if your connection is lost

Why might the wireless network in your garden center not function properly?
You failed to carry out a site survey

What is SAE?
WPA3. Simultaneous Authentication of Equals (SAE) replaces the PSK. It uses a Diffie Hellman Handshake to provide security as the password is never transmitted and is immune to offline

attacks. It also uses Perfect Forward Secrecy (PFS) that ensures that session keys are never compromised.

What is PMF?
WPA3. Protected Management Frames (PMF) uses multicast transmission and protects against IV attack.

What is WiFi Easy Connect?
WPA3. It is great for IoT devices as you can connect using a QR code.

What is WPA2 - Enterprise?
Centralised domain wireless with 128 bit encryption. It uses a RADIUS server with a 802.1x managed switch.

What is WPA3 - Enterprise?
An upgrade to WPA2. It uses 256 bit encryption and ECDHE for an initial handshake.

What is WPA3 - Personal?
Uses Perfect Forward Secrecy (PFS) which ensures that session keys are never compromised

What is WiFi Enhanced Open?
WPA3. This is an enhancement of WPA2 open authentication, where it uses encryption for open authentication. It can be used in public areas such as hotels, cafés, and airports. No password is required, and this prevents eavesdropping as it uses PMF.

What type of authentication is vulnerable to Pass-the-Hash attacks?
NTLM. It stores the password using MD4 hashes and is very insecure.

How can you prevent Pass-the-Hash attacks?
Enable Kerberos or disable NTLM. Enabling Kerberos is the best option as it uses Active Directory that stores the passwords in an encrypted database.

What type of authentication uses cookies?
Federation Services

What is TOTP?
 Timebased one-time password. Expires in 30-60 secs.

What is Federation Services?
 Third-party to third-party authentication

What protocol does Federation Services need?
 Security Assertion Mark-up Language (SAML)

What type of authentication is SAML?
 XML-based, used with Federation Services

When using Federation Services, why would you not be able to change the password for the person coming in from a third party?
 They are not in your domain or your directory services

What protocol does Federation Services use?
 SAML – an XML-based authentication. It needs cookies.

What authentication uses tokens?
 OAuth 2.0 open authentication.

What is Open ID Connect used for?
 It works with Oauth to allow internet-based authentication with an external platform such as Facebook, Google, or Hotmail.

What protocol is used by OpenID Connect?
 OAuth

What is Shibboleth?
 Open-source Federation Services executed on a smaller scale

What type of authentication uses location?
 Context-aware authentication

How many factors of authentication are you using if you use a password, PIN, and birth date?
 Single factor

What type of Federation Services connects via a wireless

connection?
RADIUS Federation. (Nothing to do with a RADIUS server; don't get them confused.)

What type of authentication does the cloud use?
Federation Services as they are third party

What are an IdP and service provider?
The person trying to access resources from a third party is known as a service provider. The person who is giving their account or token is the IdP (Identity Provider).

Where could you find date and time, as well as a list of artefacts and where they were found?
On Chain of Custody documentation

When starting a new business, you install a terminal to accept credit card payments. Which regulation should you ensure you are compliant with?
PCI DSS card payment regulations

An attacker gains access to a vulnerable guest machine, then attacks a victual SQL database. What type of attack has been carried out?
VM Escape. If it happened on a physical network, it would be called pivoting.

If domain users can log into any terminal in the building and access their desktop, and each time they retain their setting, what two technologies are being adopted?
Virtual Desktop Infrastructure (VDI) is being used to roll out virtual desktops from a pool and provide a secure desktop for contractors at short notice. The second technology is Virtual Desktop Experience (VDE). With permanent setting, this retains their settings.

What is the purpose of DLP?
To prevent PII, sensitive information, and information that has a pattern match from leaving the company by email or a USB drive.

Laptops are being stolen from a company. What can the administrator do to prevent this from happening again?
Set up geofencing or geolocation

What can an administrator do to increase the compute time for a brute force attack?
Salt the password. This appends random characters to the password.

What happens to the contents of RAM if your computer suffers a blue screen of death?
It is saved to the C drives as a dump file (.dmp) extension

What type of attack is the following: thehacker.js
XSS. It uses JavaScript.

What does ISO27701 deal with?
Privacy

What type of attack could use a well-known and trusted website?
Watering Hole Attack

Which RAID set can afford to lose one disk but provides fast-read access and has single parity?
RAID 5

Which RAID set can lose two disks and uses double parity?
RAID 6

What is 99.999% know as?
Availability (also known as the five nines)

What are Wireshark and tcpdump used for?
They are both packet sniffers, aka protocol analyzers

How can you troubleshoot a wireless access point?
With a wireless analyzer, aka WiFi analyzer, aka wireless scanner.

What type of virus cannot be detected other than by using a baseline?
Zero Day. There are no updates. A baseline is a list of applications before and after and the zero day would be the unknown.

What is the purpose of OWASP?
The Open Web Application Security Project (OWASP) is a non-profit organization founded in 2001, with the goal of helping website owners and security experts protect web applications from cyber attacks.

What is an international regulation that deals with data privacy and user rights?
GDPR. This is an EU regulation consisting of 27 countries.