Problems, vulnerabilities, risks observed after evaluating the IT infrastructure of the Network Funtime Company:

1.HR are not the responsible ones for choosing, buying or setting hardware devices

Solution: The company should have had an IT department.

2. In the company are employed software engineers, designers which need devices with better performance and better equipped (CPU, RAM etc) than the employees on the Hr and sales team. So, buying cheaper devices is not an option.

Solution: The sys admin or IT department employees have the duty to choose, buy, set up and offer to the right employees the devices. Software engineers/designer should have better PCs/laptops and better equipped devices. This can also work in favour of the company, because it will definitely help with the performance of employees.

3. No spare devices that can be used in case other fail or broke

Solution: These should always be spare PCs/laptops/Phones that employees can replace non working or damaged equipment

4. Devices are not labelled and added to the inventory

Solution: Each hardware devices used by the employees that are provided by the company should be labelled and added to the inventory. Active Directory or OpenLDAP, the centralized management tools can be used to manage users and hardware.

5. Each new purchased device is set up by the new employee

Solution: This is definitely a no-no. Users accounts, OP, software etc. is administered by a sys admin or IT employee with the use of centralized management tools or other.

6. Tech related issue are addressed to an HR employee, support is offered by the HR,

Solution: IT department should be in charge of these

9. No password management, policy or recovery plan

Solution: Active Directory, OpenLDAP

10. Existent back-up plan? no information

Solution: Back-up Plan, Disaster Recovery Plan, Post-Mortems should be implemented and documented.

Problems, vulnerabilities, risks observed after evaluating the IT infrastructure of the W.D Widgets:

1. Installation of sales-specific applications manually onto every machine

Solution1: This is time consuming, and for just for a sole IT person to do that for 80-100 users is impossible. The use of OS imaging and deployment software is the best solution to automate the installation/update process.

Solution2: Second solution is to use cloning devices or software.

1. IT-related requests are emailed directly

Solution: A ticketing system can be a good solution in this case, as the employee requesting assistance can describe the issue within a task. This is specially advised, because it is documented and everyone can see the issue and the resolution of it and can help in case this is reproducible on other machines.

1. Data is stored on a single file server

Solution: Due to the intensively growing company, the on-site hardware will soon become to less. So there should be a plan of expanding on-site, on the cloud or hybrid.

1. No back-up plan in place of critical customer data held by /created by the users

Solution: Important customer data should be kept in secure file servers with clear back-up plans, recovery plans.

1. A single person IT department

Solution: Hire more IT employees, due to the rapidly growing company.

Problems, vulnerabilities, risks observed after evaluating the IT infrastructure of the Dewgood:

1. Computers are bought from a physical store on the day the new employee starts

Solution: there should always be spare PC/laptops to use for new employees or in case other devices break. In this case the PCs are bought from a physical store, and this can imply that sometimes the product required is not in stock, and are forced to buy something else that can either be more expensive or contrary is not as performant as required

1. A single server for multiple services

Solution: different servers for critical services or some can be moved in the cloud (email). A back-up server should be in place also.

1. No messaging system in place

Solution: Slack is an instant messaging solution

1. User account not disabled in the directory service

Solution: This is important to do because of security and also can cause confusion and a lot of extra work.

1. Open-source ticketing system difficult to handle

Solution: Offer trainings for all employee, gather and document each issue and solution. Create documentation and update it.

1. Nightly backup of the file server on disk and take it home.

Solution: The back-up plan and disaster recovery plan should be more clear. In case the tape is lost, stolen or broke, there is no second back up plan in place.

1. Website on the same server

Solution: There should be a dedicated web server in place. Because all the services run on the same server there will definitely be performance issue of heavy traffic which can cause these issues. But when the problem occurs this should be evaluated, gathered information, finding the root problem, document it and present solutions.