Slide 1

Software should be updated regularly. Updates are important as they help prevent against security risks.

Problems with low level software are risky as they often go unnoticed and often can result in the biggest issues. Heartbleed is a bug in OpenSSL that allows for an attacker to gain any information stored in the memory of the target server. As well as this, ZombieLoad is an issue in Intel CPUs that allows for a program to access sensitive data that the CPU is accessing, like passwords and files. These are both issues that can be fixed through updating software.

High level software can have issues that result in similar problems, although the impacts are usually less severe. Passwords and data are still at risk, however, and keeping software updated can solve these issues.

Slide 2

Business continuity plans involve producing solutions and preventative measures for problems that a company could face. Planning and thinking about recovery methods helps lower system downtime, resulting in faster and more structured recovery. As well as this, preventative measures attempt to stop a problem from happening in the first place, identifying potential risks and mitigating them before they evolve.

Some common solutions to large scale problems are data replication, crisis management, backup sites and communication architecture planning. These all help resolve issues that could come up, like loss of communication, or data loss.