2. Based on what you learned from reviewing the 20 CIS Controls, read the scenarios below and provide the CIS Control(s) that the scenario violates, either fully or partially, as well as the risk posed by this gap.

**A. A new system is installed on the network, but not configured and patched with appropriate security updates until the following day.**

Secure configuration for Hardware and Software on mobile devices , laptops,workstations and servers.

We have to configure the new system for the latest security software update since off the box system is not secured.Zero day attack is possible because of the delay in securing the system.

**B. An administrator inadvertently opens an email that contains an infected attachment which is then used to obtain a foothold within the network for use in attacking other systems.**

Email and web browser protections

Implement a security awareness and training program

The administrator should not open an email that contains an infected attachment . Apart from email and web protections users should be trained not to open unknown email attachment.

**C. An organization has just suffered a breach and is attempting to discover how many systems were affected and identify the root cause. However, they are  unable to gather the relevant system logs which could assist them in their investigation.**

Maintenance,Monitoring and analysis of audit logs.

Enabling audit logs is important to detect the breach in the system.

**D. A company has implemented a secure email gateway to better control spam and phishing emails getting through to its users, but it’s still allowing too many to get through.**

Secure configuration for network devices such as Firewalls, Routers and Switches.

We have to properly configure the firewall so that it will not allow spam and phishing emails.

**E. A company has deployed a next generation antivirus (NGAV) solution on all of its workstations and servers, and they still got hit with an advanced ransomware attack.**

Malware defenses.

**F. A Software as a Service (SaaS) company hosts web portals to allow its auto parts customers to manage their inventories. Recently, they suffered a breach which resulted in the compromise of all of their customers' data. The root cause of the breach was determined to be a combination of vulnerabilities within their web application, namely cross site scripting (XSS) and SQL injection.**

Application software security.

Inventory and control of Software assets.

We have to test the software applications for common security weakness using a web application scanner prior to deployment.