A. A new system is installed on the network, but not configured and patched with appropriate security updates until the following day.
The Control that fits this scenario is control 5, it violates this by not updating and maintaining the software. It states in CIS control 5(Secure configurationfor hardware and software on mobile devices, laptops, workstations and servers) that by using the default configurations are used for ease of use and ease of deployment no security. By keeping on the default configurations and not patching the security updates, older protocols can be easily exploited. The Risk that is posed is that attackers have an easy way to get in since they know how to get in with the default protocols

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.
The Cis Control that this scenario violates is control 4. This scenario can also be mistaken for violating control 7(email and web browser protection) since the attacker is using the phishing method. In this case the bait is the administrator which the attacker is using to gain access within the network. The risk that is posed is the attacker is able to snag the administration privileges and have more access to the network allowing them to gain more data.

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.
This violates control 6(analysis of Audit logs). By not maintaining,not monitoring, and not having an Audit log they were not able to monitor the traffic in the network and have a detailed description of which systems were affected and how it was affected. The risk posed here was that by not knowing how the attackers got into the system, by not knowing how they got in will possibly keep it as a back door for them to get more data. Also by not knowing which systems were affected means the attacker could still be in the network passively gaining data.

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.
This violates control 7(email and web browser protection) because emails are so technically complex and flexible it allows so many that look like legitimate emails pass through that aren't real. Mainly spoofers will create content that looks like it's an administrative email with a similar email as them and it can pass through the gateway. The risk is being phished and getting breached

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.
This violates control 8(malware defenses). It violates the control because the defenses must be able to operate in this dynamic environment through large scale automation, rapid updating and integration processes. It must be deployed at multiple access points of attack to detect, and control the execution of malicious software.

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.

This violates control 3 (vulnerability management) which states cyber defenders must be updated with new info on vulnerabilities because attackers have access to this info and can take advantage of gaps between the appearance of new knowledge. Which probably allowed the attackers to inject the SQL.