**Center for Internet Security (CIS) Controls**

1. Go to the site below to see and download the 18 CIS Controls PDF, V8. Read the explanations provided for each control.

https://www.cisecurity.org/controls/v8

Then, watch each of these short, under 2-minute videos that provide an explanation as to why the control is critical.

CIS Control #1 CIS Control #2 CIS Control #3 CIS Control #4 CIS Control #5 CIS Control #6 CIS Control #7 CIS Control #8 CIS Control #9

CIS Control #10 CIS Control #11 CIS Control #12 CIS Control #13 CIS Control #14 CIS Control #15 CIS Control #16 CIS Control #17 CIS Control #18

2**.** Based on what you learned from reviewing the 18 CIS Controls, read the scenarios below and provide the **primary** CIS Control that the scenario violates, 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.

* CIS Control 4
* The system is at risk to be attacked because the security updates were not configured and patched properly there is a chance of hackers using this as a gateway.

B. A user receives an email from a sender she does not know. It asks her to immediately send a wire transfer in the amount of $50,000 to a foreign bank account for services rendered. She wires the funds without verifying if the email is authentic, only to find out that the email was a scam.

* This would be CIS Control 14 - Implement a Security Awareness program since the user would need to undergo training since they fell for a phishing scam.

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.

* Without relevant system logs there is a risk of not to be in the position to recover what was lost or find better ways to protect the system from future attacks

D. A user’s PC was infected with malware, and IT Security traced the source of the problem to an older version of Google Chrome the user was using.

* This would be CIS control 9 Email and Web Browser Protections. This is because the user is using an outdated version of chrome and updating it would fulfil CIS control 9.

E. A company has deployed a next generation antivirus (NGAV) solution on all of its workstations and servers, and they still got hit with a ransomware attack. It was discovered that the NGAV software did not have all the features and capabilities that more advanced solutions possess.

* CIS Control 7 is mostly for vulnerability management which AV's don't scan for. This would be CIS Control 10 - Malware Defences. This CIS control ensures that the AV is up to date with all the signatures to detected evolving malware.

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 would be CIS Control 16- Applications Software Security. The keywords here are "Software as a Service". CIS Control 16 ensures that the software development cycle is followed properly to maintain security. Since the root cause was vulnerabilities, this should've been caught in the testing phase of the security life cycle. Your answer would be more applicable when a vulnerability scan is done on a machine, and they want to verify.