**1. Administrative/Managerial Controls**

* [ ] Have they implemented a least privilege policy to reduce risk and overall impact of malicious insider or compromised accounts? (Preventative)
* [ ] Have they developed disaster recovery plans to provide business continuity? (Corrective)
* [ ] Have they strengthened password policies to reduce likelihood of account compromise through brute force or dictionary attack techniques? (Preventative)
* [ ] Have they implemented access control policies to bolster confidentiality and integrity by defining which groups can access or modify data? (Preventative)
* [ ] Have they implemented account management policies to manage account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage? (Preventative)
* [ ] Have they implemented separation of duties to reduce risk and overall impact of malicious insider or compromised accounts? (Preventative)

**2. Technical Controls**

* [ ] Have they installed a firewall to filter unwanted or malicious traffic from entering the network? (Preventative)
* [ ] Have they installed an intrusion detection system (IDS) to detect and prevent anomalous traffic that matches a signature or rule? (Detective)
* [ ] Have they implemented encryption to provide confidentiality to sensitive information? (Deterrent)
* [ ] Have they created backups to restore/recover from an event? (Corrective)
* [ ] Have they implemented a centralized password management system to reduce password fatigue? (Preventative)
* [ ] Do they regularly monitor antivirus (AV) software to detect and quarantine known threats? (Corrective)
* [ ] Have they implemented manual monitoring, maintenance, and intervention for out-of-date systems to identify and manage threats, risks, or vulnerabilities? (Preventative)

**3. Physical/Operational Controls**

* [ ] Have they installed a time-controlled safe to reduce attack surface and overall impact from physical threats? (Deterrent)
* [ ] Have they ensured adequate lighting to deter threats by limiting “hiding” places? (Deterrent)
* [ ] Have they installed closed-circuit television (CCTV) for both preventative and detective control because its presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions? (Preventative/Detective)
* [ ] Have they installed locking cabinets for network gear to bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear? (Preventative)
* [ ] Have they displayed signage indicating alarm service provider to deter certain types of threats? (Deterrent)