**Figure 2—Sample Incident Response Exercise Scenarios**

| Area of Focus | Scenario | Incident Identifier | Data Type |
|---|---|---|---|
| Unauthorized access | Someone has assumed the identity of an administrator and has accessed the network remotely (could be password cracking or key logging) | SIEM system | Any |
| Access, data breach | Multiple simultaneous/ongoing attacks | Network activity | Any |
| Compromise | Telecommuting compromise via social engineering | SIEM | Sensitive information |
| Computing device | Organization-issued mobile/wireless device contains malware | Vulnerability scan | Any |
| Data breach | Compromised database server | IDS | Sensitive information |
| Data breach | The backup media storage vendor has been compromised and some backup files were taken | Storage vendor | Any |
| Data breach | Ransomware has affected the system data files and backups | Malware | Any |
| Data breach | Combined cloud system provider (CSP) and SOC exercise | Any | Any |
| Network compromise | A device (e.g., router, switch domain name system [DNS]) has been found to be compromised | IDS, SIEM | Network |
| Network compromise | Someone (insider or visitor) has installed a wireless access point (WAP) into the network | System assessment | Any |
| Service | Worm and DDoS agent infestation | Antivirus software | Privacy |
| Unauthorized sharing | Sharing paper or electronic documents containing privacy information with individuals who are not authorized to access them | Supervisor | Privacy |