**Bartt Sayago – BSIT -4B 8/22/25**

[Grab your reader’s attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

***Guided Practice***

**1.What is a key strategy for maintaining cybersecurity compliance in large organizations?**

**Answer:** Automating security controls for compliance

**2.What is a key benefit of using security configuration management tools in organizations?**

**Answer**: They identify misconfigurations and monitor critical changes.

**3.What action is essential for organizations to achieve security compliance?**

**Answer:** implementing controls and processes

**4.How can organizations ensure effective security compliance?**

**Answer:** Automate security controls and continuous monitoring

**RESEARCH AND CASE EVALUATION ON AUDITING­­­­­­­­­­**

1. **SolarWind Hack**

**A screenshot of a computer

Description automatically generated**

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

**Nature of the incident**

Attackers compromised SolarWinds' Orion software, which is used for network monitoring. The breach went undetected for months, affecting U.S. government agencies and private companies.

**How auditing resolved the issue**?

Auditing tools helped identify unusual network traffic and privilege escalation. Security event logs and anomaly detection systems helped trace back the malware’s movements.

 **What audit policies mitigated the incident?**

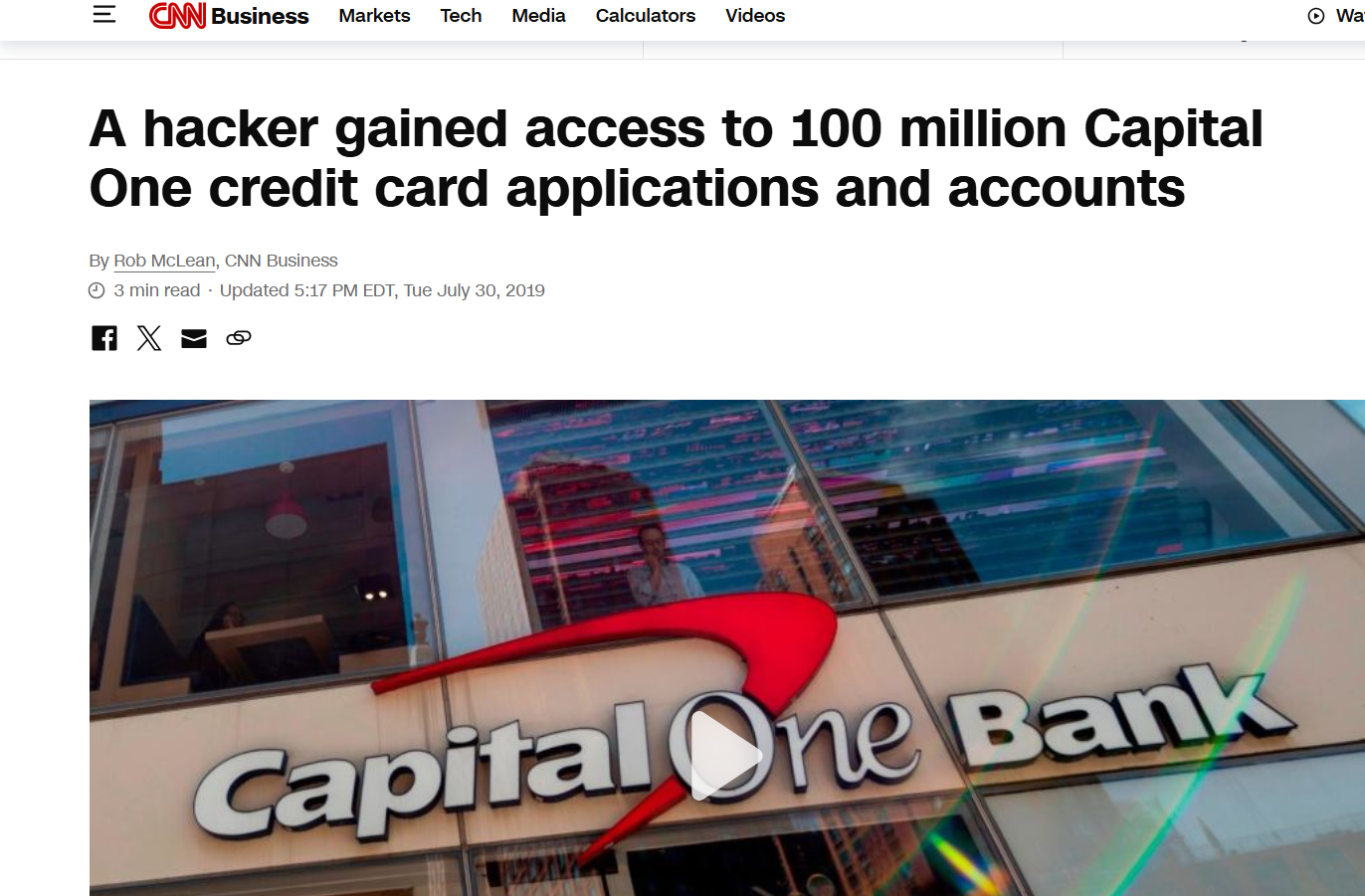
Continuous monitoring and log correlation from endpoints and network systems could have reduced detection time.

**What lessons can be learned?**

Auditing needs to include third-party vendors and supply chain components.

**­**

**2.) Capital One Data Breach (2019)**

****

**Nature of the incident**

A misconfigured AWS firewall allowed unauthorized access to cloud-stored customer data.  
A former AWS employee exploited the misconfiguration to steal sensitive information.

**How auditing resolved the issue**?

AWS CloudTrail logs were used to trace the unauthorized access and data movement.  
Alerting tools detected unusual activity, prompting an internal security investigation.

**What audit policies mitigated the incident?**

Regular audits and vulnerability scans could have identified the firewall misconfiguration early.  
Enforcing cloud-specific audit policies like IAM reviews and permission audits would have reduced risk.

**What lessons can be learned?**

Cloud environments need customized, continuous auditing frameworks.  
Proactive auditing and red teaming are essential to uncover hidden threats before exploitation.

**II.) Audit Case Analysis**

**A screenshot of a computer

Description automatically generated**

**Suspicious Activities & Why They're Suspicious**

1. **Event ID 1001 & 1002 – App Crash or System Error** The system or an app crashed unexpectedly. This could mean something is wrong or someone tried to force it to crash.
2. **Event ID 6062 – Power Problem (Kernel-Power)** Shows the computer may have shut down or restarted in an unsafe way. This might be a power issue or someone forced it to shut down.
3. **Event ID 10016 – Permission Issue (DistributedCOM)** A program tried to do something it didn’t have permission for. This can be a sign of bad settings or someone trying to bypass limits.
4. **Event ID 16384 & 1003 – Software Protection Warnings** Many quick logs from Security-SPP might mean someone is trying to mess with software licenses or system files.
5. **Event ID 7001 – Service Failed to Start** A needed service didn’t start properly. This could stop important features or be caused by someone changing settings.

**Suggested corrective measures aligned with Audit Policies**

* Turn on alerts for crash, power, or permission issues.
* Check who can change system settings or install apps.
* Review logs often to catch strange behavior early.
* Make sure software is up to date and properly licensed.