Chad Ballay

CIS411-342N

Week Four Module Two

**How would you gather and assess vulnerabilities in this case?**

Establish a baseline of how the systems behave normally. Classify the system into the taxonomy of NIST, ISO, etc… frameworks. Depending on the asset class, research best practices by using the systems framework classification to help identify likely needed changes.

<https://cve.mitre.org/>

<https://nvd.nist.gov/>

**List at least three vulnerabilities described in the case.**

*Antivirus is in use, but is not automatically updated across the company.*

This falls under two related controls. Information System Monitoring and Malicious Code Protection.

<https://nvd.nist.gov/800-53/Rev4/control/SI-3>

<https://nvd.nist.gov/800-53/Rev4/control/SI-4>

Depending on which antivirus software is in use there could also be CVE’s on the software itself.

<https://cve.mitre.org/cve/search_cve_list.html>

*Vendors are allowed access to the site and computers without authorization or supervision.*

The gate seems to be wide open. Remote Access, Third-Party Personnel Security, and Account Management.

<https://nvd.nist.gov/800-53/Rev4/control/AC-17>

<https://nvd.nist.gov/800-53/Rev4/control/PS-7>

<https://nvd.nist.gov/800-53/Rev4/control/AC-2>

*Password resets are done by giving out a generic password*

If a malicous actor can trigger a password reset then they can use the generic password to set the account’s new password to whatever they chose.

<https://nvd.nist.gov/800-53/Rev4/control/IA-5>

**Include the severity and likelihood of compromise for each vulnerability identified.**

Antivirus – Severity and likelihood are both extremely high.

Vendor access – Severity and likelihood are both high.

Password resets – Severity and likelihood are both high.

**List known or assumed safeguards in place that reduce the vulnerability's impact or likelihood**

* Weak antivirus is starting to become defacto enabled on modern OS’s. This is leading to a default posture of auto patching.
* This company being a highly specialized company in a smaller regional market probably means that the vendors it uses have long term relationships. The lack of turnover may lead to personal connection over security concerns.
* Accounts who have their password reset and then set to a chosen password of the attacker also mean that the existing workflows around them fail at that point. Users will not be able to login.

Automatic processes will begin failing. Discovery of the breach could be very timely.

**Include a list of any assumptions you are making.**

* The workplace culture is healthy enough to address employee retention and disgruntled employees are handled early.
* That this really is a niche sector. (I don’t know what an architecture firm does beyond that they deal with building design.)
* That Kansas City as a region helps further refine this company’s role as niche player in the sector. (Maybe due to some oddities in the sector Kansas City is just awash in architecture firms.)
* That users aren’t able to disable autopatching features around default AV features of the OS.
* That password resets are only done by the user requesting them as a normal process. (Maybe on the first of the month everyone’s password is reset and they have to pick a new one. Dumber processes have been implemented before.)