CIS3150 CASE STUDY

'Futura' is a large multinational banking and financial services company that works in over 100 locations internationally. Recently the company has realised that it can no longer prevent employees from using their own devices for work purposes. The company is now working to create new BYOD (bring your own device) systems and policies.

Working in the financial sector, the company are already risk averse and very security conscious. The new systems and processes must be developed and implemented whilst mitigating the risk of BYOD. Network Access Control (NAC) policies can be used to successfully implement this kind of environment, they can be used to allow, deny or grant access to devices, based on the policies set.

The company anticipates upwards of 10,000 employees using BYOD once it is allowed. The risk and compliance team at Futura are responsible for the new BYOD project. There are a number of elements they need to consider:

- Technical support requirements once BYOD is up and running
- Security and compliance issues
- Identifying a suitable NAC systems provider, tendering and choosing a suitable partner and establishing service level agreements (SLA's)
- Establishing a disaster recovery plan that ensures business continuity
- Risk assessment
- Managing the changeover process

To start the process and to give the possible NAC providers a guide, Futura have established three BYOD scenarios.

Scenario 1 — Employee-Owned Tablet/Smartphone

- A mobile device management (MDM) agent is required for the device to gain access to a wireless BYOD network.
- Employees can use any device.
- If the MDM agent is detected, the device is granted access to a separate wireless BYOD network. The system is used to grant access to a subset of applications on the corporate network, based on the user's profile, thereby creating a limited-access zone.

- If the MDM agent is not detected, the device is positioned on the guest network and is limited to Internet access only. (The user must register at the guest Web portal to gain Internet access if this occurs).
- Compromised devices such as Jailbroken iOS devices and rooted Android devices are denied access to the network, including the guest network. The MDM agent determines if the device has been jailbroken or rooted.

Scenario 2 — Employee Brings Own Windows Laptop

- Up-to-date patches are required.
- Up-to-date antivirus signatures are required (employees can select from an approved list of solutions at the company's expense, per corporate licensing agreements).
- Disk encryption is required (employees can select from an approved list).
- A secure connector agent must be enabled (checks configuration status).
- A data loss prevention (DLP) agent is required.
- If the Windows laptop is compliant with all five of the policy criteria above, it is granted full access to the corporate network.
- If a Windows laptop is noncompliant with one or more of the policies, it is positioned on the guest network and is limited to Internet access only. (The user must first register at the guest Web portal to gain access)

Scenario 3 — Employee Brings Own MacBook Laptop

- It must be running OS 10.11 or later.
- A secure connector agent must be enabled (checks configuration status).
- A data loss prevention (DLP) agent is required.
- If the MacBook is compliant with all three of the policy criteria above, it is granted full access to the corporate network.
- If the MacBook is noncompliant with one or more of the policies, it is positioned on the guest network and is limited to Internet access only. (The user must first register at the guest Web portal to gain access.)

All three of the scenarios above apply to permanent staff as well as any contractors working for the company.