

## IT Protection and Security: MIT 264

Alden A. Quiñones

### Activity 3 - Risk Assessment for BYOD Policy

---

Scenario:

Your organization plans to implement a BYOD (Bring Your Own Device) policy.

#### Security Risks Assessment and Mitigation Strategies

#	Security Risk	Description	Mitigation Strategy
1	Data Leakage	Employees may transfer sensitive data to personal or insecure platforms.	<ul style="list-style-type: none"><li>- Conduct orientation sessions on the Data Privacy Act and raise awareness about data protection practices.</li><li>- Provide training on employees' accountabilities and responsibilities related to handling sensitive information.</li></ul>
2	Lost or Stolen Devices	Unauthorized access due to misplaced or stolen personal devices.	<ul style="list-style-type: none"><li>- Enforce device encryption and strong authentication.</li><li>- Enable remote wipe via MDM.</li><li>- Require immediate incident reporting.</li></ul>
3	Malware and Untrusted Apps	Malicious apps may compromise devices and network integrity.	<ul style="list-style-type: none"><li>- Enforce the use of authorized and vetted applications only on all devices connected to the network.</li><li>- Implement Mobile Device Management (MDM) or endpoint protection solutions to monitor and control app installations.</li><li>- Conduct regular cybersecurity awareness training for personnel to recognize and avoid malicious apps.</li><li>- Regularly update software and security patches to reduce vulnerabilities.</li></ul>
4	Lack of Visibility and Control	IT cannot fully manage or monitor personal devices.	<ul style="list-style-type: none"><li>- Deploy endpoint management tools.</li><li>- Conduct regular inspections.</li><li>- Create clear usage and monitoring policies with employee consent.</li></ul>
5	Network Access Risks	Devices may connect to unsecured networks or pose threats to internal systems.	<ul style="list-style-type: none"><li>- Require VPN for remote access.</li><li>- Apply Network Access Control (NAC).</li><li>- Use VLAN segmentation and strict firewall policies.</li></ul>