TO: Senior Management

FROM: Information Assurance Lead

DATE: 2/16/2025

SUBJECT: Risk assessment & mitigation proposal

INTRODUCTION

As the company is planning on expanding internationally and engaging in licensing deals, it faces a series of new risks to its intellectual property and IT infrastructure. A significant risk is presented to the security of sales, information and personnel devices during travel. The proposal talks about the potential risks and security measures to safeguard organizations devices and network both at corporate headquarters and when the sales and marketing officers travel in the US and internationally.

RISK ANALYSIS

Threats:

1. **Theft of intellectual property:**
    - **a.** Corporate espionage by a disgruntled employee or externally by competitors.
    - **b.** Unauthorized access to confidential information during travel, client meetings and demonstrations.
2. **Device loss:**
    - **a.** Physical theft of employee's devices while traveling.
    - **b.** Unauthorized access if devices are not protected.
3. **Cyber-attacks:**
    - **a.** Data stolen during international travel due to lower cybersecurity standards.
    - **b.** Cyber-attacks targeting company employees or the company network.
4. **Legal threats:**
    - **a.** Failure to comply with local cybersecurity laws internationally.
    - **b.** Due to improper handling of client data in Europe, possible violations of data protection regulations like GDPR.

Vulnerabilities:

Vulnerabilities that should be considered to prevent possible threats. Lack of encryption, if sensitive data is transmitted between company network and devices, it can be intercepted without proper encryption. Weak authentication protocols like lack of multi-factor authentication and weak password can lead to risk of unauthorized access. During travel company employees need to refrain from connecting to external devices like USB as it can lead to exposure of company network to malware.

DEFENSE IN DEPTH STRATEGY

A defense in depth strategy is important to safeguard against the above risks. The presence of layers of security makes it hard for attackers to breach the network.

1. **At corporate headquarters:** Network segmentation allows for critical information and sensitive data to be isolated to a secure network, accessible to authorized personnel only. Access control practices through role-based access control followed by least privilege principle to enforce limited access to sensitive data. All forms of communication are encrypted to prevent data breach. Strong firewalls and IDS are put in place to monitor and block suspicious activities.
2. **During travel:** To protect data in case of device theft and loss, all devices should be encrypted. Company employees should only use secure channels to communicate such as VPNs when accessing company resources. Implementation of remote wipe capabilities in case of theft.
3. **Sales and marketing personnel training and practices:** Employees should undergo regular training related to the best cybersecurity practices, such as avoiding unsecured public networks. Practice of least privilege principle by restricting sensitive information to authorized personnel only, and this access should be logged and monitored.

LEGAL AND REGULATORY CONSIDERATIONS

With the move of company activities internationally, local data protection laws for both the US and the regions where the company operates should be complied with. Below are key regulations.

1. **General Data Protection Regulation (GDPR):** Company must ensure that all data collected, stored and transmitted to and from Europe must comply with GDPR. This includes several onerous requirements to include data breach notification, strict privacy provisions, the “right to be forgotten,” and substantial financial penalties for failure to comply.
2. **Local Data Protection Laws in North Africa:** Different countries in North Africa have different data protection laws. It is crucial to consult local legal authorities to ensure the company complies with laws when handling data in the regions.
3. **Export Control Outside US:** US government has strict laws related to export of technologies, particularly defense and encryption. The company must make sure that they don’t violate these laws when engaging with foreign clients.

MITIGATION STRATEGIES

1. **Encryption:** All company devices store and communicate information under strong encryption (AES-256) to ensure all sensitive data is protected in case of theft or breach.
2. **Multi-Factor Authentication (MFA):** All company employees are enforced to use MFA for accessing company systems and sensitive data.
3. **VPN and secure communication:** When connecting to company resources, all employees not connected to company network directly should use VPNs and secure messaging applications.
4. **Employee training and Awareness**: All employees should attend mandatory cybersecurity training, with a focus on international travel and secure device usage.
5. **Incident Response Planning:** Any form of incident should be reported with a complete incident response plan related to theft of device, network breach, and unauthorized access.

CONCLUSION

For successful expansion of the company's operations internationally, the company needs to address possible risks associated with intellectual property and IT security. A multi-layered security approach is crucial to safeguard devices and networks. The above proposal should be followed to minimize potential threats, safeguard against legal troubles, and protect their assets both at headquarters and while travelling.