Memo

To: Senior Management

From: Jack Gubasta (Cybersecurity Operations Lead)

CC: Overseas Sales Team

With sales reaching a record high and plans to expand into European and North African markets. It is essential for the organization to understand potential risks and cyber threats they may encounter overseas, and how to properly mitigate them. This memo contains a defense in depth strategy to protect the organization's data and assets overseas.

Defense in Depth involves using a layered security model to protect an organization.

data from being compromised. A layered security model involves using multiple security controls to protect data, meaning if one layer of security fails, there are multiple fallback controls. For our overseas sales and marketing teams this means protecting company assets such as company laptops and mobile devices.

Protecting laptops & mobile devices:

1. **Pins & Biometric locks**: On top of a 4-digit pin number, all company devices must utilize a biometric authentication method. This could be done using a fingerprint scanner or face ID native to all company devices to ensure that if stolen an attacker cannot access the data regularly. The combination of a pin and biometric lock provides device with 2FA (2 Factor Authentication.)

2. **SED (Self-Encrypting Drives):** All company devices must use a Self-Encrypting Drive. SED's encrypt data on the fly without user interaction. They offer strong security without impacting device performance significantly.

3. **Secure Stolen Assets:** Every company device needs to utilize an SED that supports secure erase capabilities. Secure erase capabilities provide a way to remotely encrypt/ overwrite all data on a device. If an employee loses a device, it should be immediately reported to the IT department to prevent unauthorized data exfiltration. Any employee who fails to report a lost device may be subject to reprimand.

Training Employees to Improve Security Posture: Arguably the best way to ensure data is protected is by ensuring all employees understand the risks associated with traveling overseas with company assets. Employees must be mindful of where they are using company devices and how they are using it. I purpose a mandatory 3-day course covering proper use of company devices as well as understanding social engineering techniques and foreign threat actors

Day One: Using Your Company Device Securely: Day one of my training regime will first cover the devices AUP (Acceptable Use Policy.) This includes how to properly set up the appropriate locking devices, websites that are not authorized for visitation, and avoiding public Wi-Fi networks, such as in an airport or Café.

Day Two: Understanding Social Engineering: A huge portion of data leaks happen as the result of a social engineering attack. Social Engineering are tactics used by attackers to get authorized users to divulge sensitive information or install malware unwittingly. Social engineering techniques can include pretexting, prepending, phishing, baiting, and other techniques should be fully understood by all employees to avoid a serious security incident.

Day Three: Foreign Threat Actors: All employees must understand hacker groups and their TTPs located in the regions they will be operating in. For example, this includes hacker groups such as Fox Kitten, who are known to operate in North Africa. Employees traveling to Europe should also be mindful of the slew of hacker groups which operate in Europe. The MITRE ATT&CK website hosts a list of known hacker groups and their TTPs. Which can be found here: https://attack.mitre.org/groups/

Conclusion: In a time when our organization is seeing record profits it becomes clear how important it is to ensure company assets and data are protected. Data breaches can cost an organization potentially millions of dollars. By using a layered protection model and ensuring our employees demonstrate cybersecurity competency, we can prevent data breaches.

A data breach can have serious effects on the organization's monetary value (particularly in European markets due to the GDPR law which requires a company to pay 20 million Euros, or 4% of the company's annual turnover to the victims.) On top of monetary value, a data breach can have serious negative effects on the organization's overall reputation. It is for this reason we must layer our security, and properly train all employees traveling to foreign markets.