Unit 2: Governance, Risk, and Compliance

Deliverable 1: Measure and Set Goals

Potential Security Risks

There are a number of potential security risks that may evolve when employees are allowed to access work information systems from their home and on their own personal devices. The risks may include[1];

1. **Data Leakage**; which may be unintentional and may occur through the board permissions set on various third-party applications that have been downloaded on the mobile device. Most likely these are the free apps that are available on the various app stores, which may perform as advertised, but also send personal—and potentially corporate—data to a remote server, where it is mined by advertisers, and sometimes, by cybercriminals. Data Leakage may also happen through malware infused enterprise sign-in websites that may look legitimate but are actually stealing information.
2. **Unsecured Wi-Fi or Network Spoofing**; When employees are working on their mobile devices they need to be especially careful if they are accessing free public Wi-Fi networks as they are the most vulnerable to cyber breaches since they are usually unsecured. The biggest threat to free Wi-Fi security is the ability for the hacker to position himself between you and the connection point, instead of talking directly with the hotspot, you're sending your information to the hacker, who then relays it on and in that wy hacker may access any info you are either sending or receiving over the Wi-Fi. Hackers may also plant malware in free Wi-Fi connections, prompting pop-ups which when clicked may install malicious software on the device. [2]
3. **Phishing Attacks**; Phishing attacks are when employees open spam emails which may look as if they are from legitimate sources but aren't and have some sort of malicious code on it which may steal credit card, passwords and banking info, and if are able to gain access to company network through the mobile devices may embedded malicious coding there too. Since mobile devices are always powered-on it makes them more vulnerable to phishing attacks through emails since people look at their emails in real-time on their phones , opening and reading them when they receive it.

---

[1] Kaspersky. (2020, March 31). Top 7 Mobile Security Threats in 2020. Retrieved May 31, 2020, from https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

[2] Kaspersky. (2019, January 31). How to Avoid Public WiFi Security Risks. Retrieved May 31, 2020, from https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Preferred Employee behaviour to security risks

Preferred employee behaviour to the above threats would be to have a general understanding and awareness of the cyber threats that are there. Keeping in mind that anything can be broken into and we as employees need to be vigilant.
To avoid **Data Leakage**, only give apps the permissions that they absolutely need in order to properly function. And steer clear of any apps that ask for more than necessary permissions. Make sure that your mobile operating systems are up-to-date be it ios or android.
To avoid **Unsecured Wi-Fi and Network Spoofing**, use free Wi-Fi sparingly on your mobile device. And never use it to access confidential or personal services, like banking or credit card information. Never provide personal information. And whenever you are asked to create a login, whether for Wi-Fi or any application, always create a unique password.
To avoid **Phishing Attacks**, Set up multiple email addresses, have a separate email address for just public wi-fi access. Never respond to any spam and be vigilant about the spam emails, look at the web addresses carefully for legitimacy, or think about why you received them. Use anti-spam filters on your email.

Methods to measure employees are following guidelines

Some methods to measure this success are;

1. Conduct Surveys; monthly or bi-weekly asking employees about what type of email they open, when, what to do they look for when identifying spam, or ensuring the Wi-Fi is secure.
2. Conduct pen test demos at random
3. Screen and monitor employees; not just during the hiring process for malicious intent and casual nature but make sure once they are on board and deal with sensitive information that they are told that their logins will be monitored.
4. Have policies in place for mobile phone use and logins that every employee needs to have antivirus and anti-malware softwares installed, require employees to report lost or stolen devices immediately and provide disk encryption on mobile phones.
5. Educate employees through awareness and training every bi-weekly or monthly basis.

Goal

The ultimate goal of the organization would be to reduce the amount of data breaches, leaks, malware and phishing attacks through employee mobile devices and a goal of less than 5% breaches per month or year should be looked at.

Deliverable 2: Involve the Right People

Now that we know what our goal is we need to put in place the right team to lead us to the goal.

It is very important to have the right people in place. I feel there should be a dedicated Cybersecurity team working as a full-time function within the organization , not just as consultants especially in those medium to large companies that have a large number of employees who have access to the company's information system on their mobile and remote devices.
The personnel i would have would be;

1. Chief Cybersecurity Officer (CCO) - Standalone with dedicated staff including security architects, hackers, pen testers working under him
2. Chief IT Officer/Department - Have a separate IT department with its own budget, responsible for any IT hardware, software, network issues.
3. Dedicate liaison specialists/leaders(VPs) who represent every other department and who negotiate on behalf of their respective department heads when dealing with cybersecurity issues , budgets and decisions. E.g TD Bank - VP Liaison Business banking, VP retail banking & H.R. may represent their own departments in front of the CCO and CIO/IT department.
4. Trainers; leveraged from Cybersecurity and IT departments to conduct training sessions.

Deliverable 3: Training Plan

I would look to implement a bi-monthly training. Which would be a combination of in-person through seminars and demonstrations. But also online, be using learning tools and in-corporating surveys, online courses with mandatory completion requirements.Give your staff a clear channel, such as an emergency number, to alert your administrator to any suspicious emails or unusual activity, or for reporting a lost device – even if it turns out to be a false alarm. Some cyber-attacks are preceded by a seemingly innocent work-related phone call, purportedly from a supplier or service provider to establish account details or passwords, so don't overlook the significance of such calls as a precursor to cyber-crime. If an attack or breach does occur, give everyone a timely heads-up to limit the impact of the attack. Ensure you have an internal communications plan and PR strategy in place should the worst happen so your teams are equipped to field questions and reassure concerned customers or investors.
Topic covered in the training can be;

- Malware
- Wi-Fi networks
- Mobile security
- How to recognize Email scams and phishing

- Safe browsing rules
-

While there's no foolproof method to protect your business, educating your employees about security threats and best practices for online behavior and privacy can at least reduce the likelihood of a breach caused by human error.

MEASURES TO ENSURE COMPLIANCE

1. TOP-DOWN LEADERSHIP BUY-IN; LEaders taking a charge and leading by example
2. Periodical security assessments

Other Solutions

Administrative controls like monitoring data logins by managers and email monitoring, this can serve as a deterrent. Advantage can be that the employee can be reprimanded within its departments through his direct boss leading to less embarrassment. Disadvantage is the privacy of the employee.

Physical control, giving secured dedicated devices to employees for remote access. Advantage of which is that it would be fully encrypted. Disadvantage could be when it's lost or stolen and has to be replaced.