Cybersecurity

Assessing Security Culture

Step 1: Measure and Set Goals

1. Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.

1) The employee could download a mobile game that is malware infected. The next time the employee logs into the company database, they may end up transferring the malware into the company network.
2) The employee might be in an airport, and need to send a file. If they’re using their personal device without a VPN or hotspot from their corporate network carrier, they may be a victim of a man in the middle attack, and connect to someone’s pineapple that has “Pearson Airport” as their SSID.
3) The employee’s personal phone might be physically stolen. You could argue this is equally likely with a company phone, however, by having access to company data on the personal phone, you have another entry point for any would-be attacker into SilverCorp’s system.

   Source - https://resources.m-files.com/blog/the-top-7-risks-involved-with-bring-your-own-device-byod-3

2. Based on the previous scenario, what is the preferred employee behavior? (For example, if employees were downloading suspicious email attachments, the

preferred behavior would be that employees only download attachments from trusted sources.)

I’m going to preface this by saying employees shouldn’t access company data from their personal device (as is my company’s policy) but I will outline preferential behaviour below:

1) Be careful about the games you download. Only download games from developers you know and trust, and make sure the games are updated so the likelihood of zero-day vulnerabilities or other exploits are patched is higher.
2) To avoid a man in the middle attack, I would discourage employees from connecting to open public networks. Only connect to networks you trust.
3) To reduce the likelihood of your phone being stolen, I would tell the employee to not leave their phone unattended in public, and to make sure to check the back of the airplane seat before they depart. Knowing the physical location of your device at all times is the best way to mitigate this risk.

3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior? (For example, conduct a survey to see how often people download email attachments from unknown senders.)

1) Monitoring employee downloads on their personal device isn’t possible due to privacy concerns. However, you could measure the amount of monthly training the employee does on the risks associated with downloading programs and educating them on how networks get infected with malware. If SilverCorp isn’t already, I would be informing the SOC to monitor for malware as well.
2) You could measure the amount of time the employee is connected to the company phone’s hotspot (if each employee has a company phone in addition to their personal phone). Otherwise, you could monitor the amount of time the employee’s phone is connected to public networks, but again, this isn’t likely feasible due to privacy concerns.
3) You could assign an airtag to their company phone that corresponds to their personal device, and monitor the location of their device. So, you could measure the amount of time the employee’s phone is online through the airtag service.

4. What is the goal that you would like the organization to reach regarding this behavior? (For example, to have less than 5% of employees downloading suspicious email attachments.)

1) No malware infections into the company network.
2) Reduce employee tendency to connect to open networks. Aim for employees to be on the company phone’s hotspot 50% of the time unless at home, where presumably the home wifi is safe.
3) Reduce lost devices by employees to only 3 per year.

Step 2: Involve the Right People

5. List at least five employees or departments that should be involved. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.

1) Cybersecurity Architect - Have them design the network in a way where any malware infiltrating from employee error (via slack or outlook) is met with multiple firewalls. This will hopefully slow down the malware infection so it can be dealt with by blue team personnel.
2) Chief Risk Officer - brief them of the security plan. Obtain feedback and get buy-in so other C-Suite executives approve the plan.
3) HR - have HR track compliance with training modules (for malware infection, man in the middle and lost devices) so employee compliance is being tracked.
4) Incident Response - have them focus on suspicious activity in the network. Have them hold daily briefings to keep the urgency and awareness of malware threats at the front of their minds.
5) CFO/financial decision maker - Present the cost of the training plan and communicate cost savings via averted breaches. Makes them forecast a budget for cybersecurity training over coming years, to avoid sloppy behaviour from employees.

Step 3: Training Plan

6. How frequently will you run training? What format will it take (e.g., in-person, online, a combination of both)?

1) Malware training will run quarterly, and be online modules.
2) Middle in the man attack will be demonstrated, in person, twice a year. On these days, IT and security staff will promote a “Security

first" culture to the staff and present demonstrations on how man in the middle attacks work.

3) Quarterly online training modules will be run to show the employee the effects and likely spots, that their device may be stolen.

7. What topics will you cover in your training, and why? (This should be the bulk of the deliverable.)

1) The malware training will contain content about what it is, and why infection through a personal device will put company data at risk. They will be informed of the 5 major types of malware, and how to identify them. The employees will be informed that malware is the most frequent form of cyberattack.The employees will also become aware of the costs associated with malware infection, which runs close to $1 million for large businesses. The goal is this training is preventative, since malware infection is detrimental to an organization's business operations.

   https://teachprivacy.com/malware-training/

2) The employees will learn what a MITM attack is, and likely places this attack could occur. They will be informed about how MITM is usually used for information gathering, and if targeted, subject themselves and the company to larger attacks. Case studies will be reviewed to give the employees context, so they can picture how easily these things can happen. They will learn that financial institutions are a target for attackers. They will learn that a MITM has the following steps: Interception and Decryption. They will become aware of the major forms of decryption, such as: IP spoofing, ARP cache poisoning, DNS spoofing, HTTPS spoofing etc. This will hopefully spark a debate, and interest, among the employees and then the presenter will explain the decryptions. The goal of this training is preventative,so that employees can identify locations that are dangerous, and change their behaviour accordingly.

   https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

3) The online modules will contain information regarding likely places a phone will be stolen (airport, gym, mall etc). The goal of this training will be to raise a general awareness about the threat of malicious actors looking to steal their phone, and discuss theft prevention strategies. The goal of this training is preventative.

8. After you’ve run your training, how will you measure its effectiveness?

Outcomes of the training will be measured against the goals recorded in Question 4. If certain employees are repeat offenders, extra training will be administered.

Bonus: Other Solutions

9. List at least two other potential solutions. For each one, indicate the following:
    a. What type of control is it? Administrative, technical, or physical?
    b. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
    c. What is one advantage of each solution?
    d. What is one disadvantage of each solution?

An alternative solution that I would propose is not allowing employees access to company information from personal devices. This would be an administrative (new policy would be a company issued device) and technical (access denial to company information via firewall etc). This control is preventative. An advantage of this solution is that the risk of an employee subjecting the company’s data to attack via personal device access is zero. A disadvantage is the cost associated with issuing devices to every employee.

Another solution is to install some endpoint protection, specifically, endpoint detection and response (EDR). This is a technical control, with the goal of detecting possible security incidents. An advantage of this control would be greater visibility to threats aimed at corporate data. A disadvantage would be the cost associated with implementing EDR.

https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/