Week 2 Homework

Leo Katz

### 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.

There are a multitude of security risks that come about as a result of employees using personal devices for work activities--whether this comes about organically, or as a result of a formal Bring Your Own Device policy.

1. One such is spyware, which finds mobile devices as ripe targets according to Martin Gontovnikas.
2. Another is man-in-the-middle attacks. Users may connect, sometimes unwittingly, to unsecured public wifi, which can then expose confidential information.
3. Finally, mobile devices can be lost or stolen. Roman Foekl of CoSoSys reports that “...sensitive data [can be] compromised by an employee leaving a mobile device at a restaurant and not reporting it lost…”

Sources: [1](https://www.esecurityplanet.com/mobile/mobile-security-threats/) [2](https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/) [3](https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/)

2. Based on the above scenario, what is the preferred employee behavior?

The preferred employee behaviors would be:

1. Secure all mobile devices used for company purposes with two-factor authentication, or at least biometrics.
2. Never connect to public or even home wifi networks without using the corporate VPN.

3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?

The first item could be accomplished by spot-checks, but this may seem invasive depending on how it is administered. The second item is more difficult to track, but I imagine a filter could be put on the company servers to reject (or at least track) connections not from the corporate intranet or VPN.

4. What is the goal that you would like the organization to reach regarding this behavior?

The twin goals would be to ensure 100% use of two-factor authentication and 100% use of VPN.

### Step 2: Involve the Right People

* CEO or COO
  + In a typical corporate structure, all authority flows from the top downwards. For a smaller company, one might go directly to the CEO for authorization to engage in new security measures and training. For a larger one, the COO would be a more appropriate contact.
* Human Resources
  + Since the responses will inevitably involve training, Human Resources (HR) must be consulted. They will assist in setting aside employee time, meeting space, and other resources necessary for training.
* Legal
  + What standards can we reasonably hold our employees to? How much control can we exert over personal devices, given that they are used for corporate purposes and can contain sensitive data? These are questions best answered by the Legal Department.
* CFO
  + Adjustment of security standards and training therefore takes time and resources--both of which equate to money. There will undoubtedly need to be coordination with the CFO or other members of finance in order to justify and set a budget for this project.
* CISO and/or CIO
  + In the given scenario, it is somewhat unclear what my relationship is with SilverCorp. Perhaps I *am* the putative CISO. Perhaps I’m merely a consultant. Regardless, it is absolutely imperative that the Chief Information Security Officer and the Chief Information Officer are both consulted. The matter at hand is, after all, securing corporate data.

### Step 3: Training Plan

* Training Course A will be in person and focused on multi-factor authentication (MFA) for mobile devices.
* Training Course B will be remote and focused on the proper setup and use of the corporate VPN.
* The employees of SilverCorp will be divided into 5 equal, heterogeneous (mixed departments) groups
* These groups will be labelled, for the sake of ease, Group 1, Group 2, Group 3, Group 4, and Group 5
* During the first or second week of a given month (depending on scheduling from HR), a group will undergo Training Course A.
* The in-person Training Course A will be accompanied by a small treat or reward--e.g. free donuts.
* During the third or fourth (see above qualification) week of a given month, the same group will undergo Training Course B.
* During the first or second week of the following month, the same group will be quizzed and spot checked about the proper use of both MFA and VPN.
* Employees who perform well on the quiz/check will be rewarded with another small treat.
* Employees who do not perform well on the quiz/check will try again during the third or fourth week of this second month. Similarly, they will be given positive reinforcement via a treat.
* This will proceed in a staggered fashion until all employees are trained and checked within two quarters. See Table 1 and Table 2 for further details.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Q1.1, Jan | | Q1.2, Feb | | Q1.3, Mar | |
|  | Weeks 1&2 | Weeks 3&4 | Weeks 1&2 | Weeks 3&4 | Weeks 1&2 | Weeks 3&4 |
| Group 1 | Train MFA | Train VPN | Test | Remedial Test |  |  |
| Group 2 |  |  | Train MFA | Train VPN | Test | Remedial Test |
| Group 3 |  |  |  |  | Train MFA | Train VPN |

Table 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Q2.1, Apr | | Q2.2, May | | Q2.3, June | |
|  | Weeks 1&2 | Weeks 3&4 | Weeks 1&2 | Weeks 3&4 | Weeks 1&2 | Weeks 3&4 |
| Group 3 | Test | Remedial Test |  |  |  |  |
| Group 4 | Train MFA | Train VPN | Test | Remedial Test |  |  |
| Group 5 |  |  | Train MFA | Train VPN | Test | Remedial Test |

Table 2

Topics for Training Course A:

The focus of Training Course A will be multi-factor authentication, abbreviated as MFA.

* Introduction with a nearly universal MFA experience--swiping a bank card and then entering a PIN
* General explanation of MFA and its advantages. In my experience, people are much more willing to go along with a certain procedure if they understand its use. Back this up with statistics.
  + Two-factor authentication is one of the top three things that security experts rate among online safety practices per [Google Security Blog](https://security.googleblog.com/2015/07/new-research-comparing-how-security.html)
  + MFA is more secure than a password according to [Microsoft](https://www.microsoft.com/en-us/security/business/identity-access-management/mfa-multi-factor-authentication)
* Walk employees through setting up MFA on their mobile devices
  + <https://www.lifewire.com/why-you-should-embrace-ios-15-built-in-mfa-5189053>
  + <https://agritech.uark.edu/help_support/knowledge_base/mfa_android.php>
* Take questions, distribute treats, and conclude training.

Topics for Training Course B:

The focus of Training Course B will be the setup and use of the company’s Virtual Private Network, or VPN.

* Introduction with innocuous questions about mobile device habits.
  + Who has worked from home?
  + Who has worked from a coffee-shop?
  + Who has worked from an air-port?
* Describe man-in-the-middle attacks and other dangers of unsecured wifi networks.
* Explain Virtual Private Networks and how they establish virtual point-to-point connection, which increases functionality, management, and most importantly security.
* Guide employees through installing and using the company VPN. I cannot go into too much detail here, as I do not know the specifications of SilverCorp’s VPN.
* Take questions and conclude training.

After all of the training and evaluation/reinforcement sessions have taken place, finally in Q3 we can measure the effectiveness of our courses of action. As previously discussed, we will take measurements in two different ways for our two different controls. For MFA, spot checks among employees at a rate of 10% per quarter should be sufficient to keep the practice universal. For VPN, the company servers can be set to refuse outside traffic not originating from the VPN. This both encourages VPN use by making it indispensable to work remotely and also adds another layer of security for SilverCorp. Once more, we are aiming for 100% compliance with these two new controls.

### 

### Bonus: Other Solutions

1. Provide company-issued and controlled devices for remote work.
   1. This is a combination of all three control types. Administratively we forbid the use of personal devices. Technically we format and secure these devices exactly as needed, update them regularly, and prevent the download of unauthorized apps. Physically, we can ensure that these devices include biometric security measures as an added layer of protection.
   2. This control is preventive, as it rigidly restricts employees from making many (but not all) security breaches.
   3. This solution maximizes the control and security of SilverCorp when it comes to remote work.
   4. This solution is tedious, expensive, and requires a large amount of technical resources to both set up and maintain.
2. Best-Practices Mobile Security Training
   1. This is an administrative control. No new technical or physical controls are implemented; employees are simply instructed to refrain from using public networks, reusing passwords, and so on.
   2. This control is compensating. It aims to improve security purely through the actions of the employees, not through improved security measures.
   3. This solution is likely the cheapest.
   4. This solution is also likely the most unreliable, as the human factor is one of the most volatile and dangerous ones in the realm of security.