Step 1:

1. One of the major security concerns with remote work and employees using their personal devices for work-related purposes is how quickly issues can be resolved. “According to [the Velocity Smart Technology Market Research Report 2021](https://www.velocity-smart.com/en-gb/velocity-smart-technology-market-research-report-2021), 70% of remote workers said they had experienced IT problems during the pandemic, and 54% had to wait up to three hours for the issue to be resolved” (https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home

Irwin, 2021, p. 3).

Another great risk from remote work is that there is a lack of cyber security precautions in home versus in the office - such as firewalls, restricted IP addresses, and the ability to ensure employees are using only work issued devices for work related things.

Phishing is one of the most obvious and most prominent attacks that can be carried out in these situations. Irwin writes that “A recent report found that there has been a [600% increase in reported phishing emails since the end of February](https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/)” (Irwin, 2021, p. 17).

Another attack that can be carried out is packet sniffing against unencrypted data and files. While “companies may think to encrypt data that’s stored on their network, they may not consider encrypting data when it’s in transit from location to another,” allowing that information to be intercepted by threat agents (https://www.soscanhelp.com/blog/remote-work-cyber-security-risks

Kastner, 2021).

Through my own experience, I know that remote workers are much more likely to work from a variety of places - whether that be a coffee shop, a friend’s house, or an AirBnB on vacation. All of these places, however, provide a WiFi connection that has a high probability of being unsafe to use while working. This puts the employee at a higher risk of connecting to an unsecure network, opening it up for man-in-the-middle attacks.

1. The preferred employee behavior for the scenario provided would include:

* Only checking their work emails/Slack notifications on their work-issued devices, not on their personal devices
* Not using personal computers or phones to relay information, open or send work files, etc
* Limiting work related activities to the “normal” or “regulated” working hours established by SilverCorp

1. In order to measure how often employees are not engaging in the preferred behavior as described in the scenario, options could include:

* Sending out a survey asking what hours they typically work throughout the day
* Sending out a survey asking how often they engage in work related activities, such as checking their emails etc., on personal devices as opposed to work issued devices
* Sending out an email with which IT can see where it was opened (whether that be the location, the device, etc)

1. The goal for the organization regarding the preferred behavior would be:

* for less than 5% of employees to use their personal devices for work related issues
* for employees to use unknown/unsecured network connections less than 10% of the time

Step 2:

The involved parties in this scenario, in order to reach the goal, include:

* The HR department
  + This department would need to send out the surveys to the employees and ensure that all of the surveys are filled out and returned promptly
  + After the data is collected from the surveys, this department can report the information to the rest of the team
* Chief Information Security Officer
  + Help to plan and manage the process
  + Communicate the importance and necessity of the goals and the severity of the current employee behaviors
* The employees
  + While it may assumed that employees should not be informed since they are being “tested,” I believe that letting the employees know the current issues and roadblocks that the company is facing, it allows for
    - A higher chance of employees understanding the severity and being willing to fix it
    - A stronger argument for punishing those employees who choose not to take it serious
* Legal Team
  + Legal counsel is important both during the data collection and training, in order to ensure that the organization is following protocols and regulations, and after - making sure that if the organization has to punish any employees, they are safe to do so
* An outside organization that can create and implement training
  + The training should be based off of the specific issues the organization is facing
  + Create and implement training both online and in person

Step 3:

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

* Training will be both in person and online. Online training will be sent out monthly in both the form of videos and quizzes. In person training will be held quarterly at an off-campus site such as a community center or event center. In order to make the training more bearable and encourage employees to pay attention and take it seriously, there will be various quizzes throughout the training that must be passed in order to complete the training. In addition, the following will be provided to the employees present at training:
  + Coffee and other beverages
  + Catered lunch
  + Snacks

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

* Training will cover various forms of cybersecurity threats. A basic overview of how cybersecurity works - think WiFi connection, routers, etc. - will allow the employees to have a little background information prior to the rest of the training.

Phishing will be covered in every training. This will include the different ways that phishing can look such as: emails from legitimate businesses (PayPal, Netflix, Amazon, etc.), urgent emails from addresses that appear to be someone you know (a boss, colleague, family member, etc), a phone call from what seems to be a legitimate company, etc. This part of the training will be amended every time and reflect the current “popular” phishing attacks.

* Training will also cover the dangers of working on unsecure devices (personal devices) and unsecure networks (WiFi at the coffee shop down the street, hotel Wifi, etc). I believe it is safe to assume that most employees do not currently see the danger in this, and instead think that they are actually being great employees by still working while they are away from home, on vacation, etc.
* In addition, training will include how to know if you are on a secure network, how to secure your own network, and the safest ways to work from home/out of the office.
* The IT team will also implement a “phishing email” button, similar to a “spam” button, that employees can click on when they open an email that appears to be a phishing email. Clicking this button will send the email to IT so they can look at it. The training will include reminders on where to find this button and when to use it. (the police department i work at has this implemented and I am a huge fan).

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

* The effectiveness of the trainings will be measured by how often employees click on links in IT-sent Phishing emails after the trainings vs before the trainings.
* Sending out an anonymous survey every quarter asking how often employees have done work related tasks on personal devices.
* Similar to the above survey, an anonymous survey asking how often employees work while connected to an unknown WiFi source.

Step 4:

Two other potential solutions:

1. Providing every work-from-home employee with a WiFi network router that has company-approved safety precautions already in place
   1. This is a mix of administrative, technical,and physical controls
   2. This control has a preventative goal
   3. An advantage to this solution is that as long as employees are connected to this WiFi while they are working, there is a stronger chance that the data/work they are using will be protected.
   4. A disadvantage of this solution is that it is expensive, and there is no guarantee that employees will work only while connected to this WiFi.
2. Pre-downloading the necessary applications and programs on employee work-issued devices and not allowing those applications and programs to be downloaded onto any other devices (or, if they can be downloaded, they can’t be logged in to using the company credentials).
   1. This is an administrative control.
   2. This control has a preventative goal.
   3. An advantage of this solution is that it prevents employees from exposing sensitive information to threat agents by taking away their ability to use personal devices for work-related tasks.
   4. A disadvantage of this solution is that productivity may go down drastically if employees cannot use their personal devices.