Step 1:

* 1. One possible risk of employees using their personal phones to conduct work is that they could download an app/game on their phone with hidden malware that could infect the companies systems.
  2. Another risk is that they are not always on a secure network so it puts company data at risk of being stolen.
  3. If an employee opens up a phishing email on their device, even if its a personal email, and it’s connected to companies systems or accounts it could introduce whatever virus or attack that was hidden in the email to company systems

1. With the above the preferred measure would be for employees to not use their personal devices to conduct company business. If it were absolutely necessary for them to conduct work-related tasks on their personal device it would be preferred for them to do so on a secured network with proper protections on and not opening suspicious emails.
2. Some methods to measure how often people are not adhering to above are to send out anonymous surveys or questionnaires so employees are more likely to answer truthfully. Another is to send out false phishing emails that track to see the number of employees that would open a suspicious email.
3. Ideally the goal would to have no employees using personal phones to conduct work related activities or open suspicious emails/downloading links with a possible threshold of roughly 4% or for the company to give certain staff company cell phones that they can preform company business on

Step 2: People/Departments

1. HR: The HR department/person would need to get involved to determine if the measure is ethically/legally acceptable to run. They would also need to be involved with any disciplinary measures that might result.
2. PR/Marketing: They would have to look at the public image of the company and how taking measures might affect the company's image (e.g. the company that sent out a phishing email promising a bonus to employees). They would also probably want to use the possibility of increasing the security as a selling point.
3. IT: The IT department would have to get involved to set up the measures and compile the data. They would also have to set up protections for those that are still opening suspicious emails and links. Also if the company decided to implement company cell phones, they would have to set up the phones and make sure the proper firewalls and securities are on the cell phones and all up to date.
4. Accounting: Going off SilverCorp introducing company phones to individuals they would have to look at the cost of getting the devices and monthly cost of the plans. They would also have to look and keep a record of how much financial loss would occur if their system were to be compromised and the finances were attacked or even how much the company could afford if ransomware were to make it on their system.
5. Department heads/managers: They would need to ensure that their employees are adhering to the policies of not using personal devices for company business. One way would be to monitor when people are emailing and comparing it to when they are on the clock, also for indicators of devices sent from (some devices will add messages like “sent from iphone”). Also to ensure that employees are attending/completing proper training.

Section 3: Training

Employees would go through a set of training to go over the risks of completing work related tasks on personal devices and other security risks. This training would be a combination of in-person and online depending on which training and time frame of employment (i.e. new hire vs veteran employee). The timeline of these training sessions would depend on topic covered and employee adherence. The overall goal of employee training will be to inform them of risks involved with using their personal devices for work and work devices for personal reasons along with overall cyber security risks.

A combination of both in-person and online training would allow for a complete training experience allowing employees the freedom to complete within a certain timeline but also conveying a sense of importance especially with the in-person training. More imminent topics that would require demonstrations or for new hires would be conducted in-person to better insure employee retention of information. Online training would help mitigate the overall cost of training (according to chron, online based training can save up to 75% on training costs).

Initial hire or implantation of the training is going more frequent in the beginning with the hope of moving towards ever 4-6 months. Based on research, Gordon Flesch Company suggests 4-6 months based on employee retention and importance of training. If training is left with too large of a gap in between employees might forget training and revert back to past behavior. If training is too often employees might get over inundated with information and cut down on actual work time.

One topic of training would be on identifying phishing emails and their risks. This will give employees an idea of what common phishing emails look like and how they will possibly harm the company. Phishing emails are one of the more common attacks on companies with how many employees will click or open them without thinking. The idea is that this will be one of the training that will occur every 4-6 months to train employees to better identify the phishing emails and not open them.

A training on the possible harm of completing work on an unsecured public network would also be covered. On public networks it opens up all sorts of threats to easily access sensitive information. In most cases places with public wifi typically do not have proper securities in place that can allow a number of attacks to occur. Whether it's a man in the middle attack to slipping malware onto a system through the wifi it's just not a good idea to complete work on public networks and this training would cover precautions employees can take on these networks or the importance of not completing company business on said wifis or bringing company devices on to the networks.

If SilverCorp decided to give company phones to certain employees they should go through regular training on proper use of this technology. Training would include how it is unsafe to use those devices for personal use and how it could damage the company. If an employee started downloading different apps or going to certain websites on the company phone they could run the risk of malware being hidden somewhere in the app or website. If there is malware that gets on the cellphone and that cellphone has company specific apps or logins it could get into the network and infect the whole system. So this training would go over the risks of using company cell phones for personal use and go over proper usage of this technology.

It would also be a good idea for SilverCorp to have a training on proper password management. This would cover what defines a good password, how often employees should change their passwords, and the dangers of writing down their passwords. If employees are still using personal phones for business related work they should try to use different passwords and this would go over why this is important and the risks of having similar passwords (if hackers get one and the rest are alike its easier for them in attacks.)

I think that there are a couple ways to test the effectiveness of training including surveys/questionnaires and test phishing emails. I feel that if surveys/questionnaires are done anonymously employees are more likely to give honest feedback rather than attaching identifying information if they are not adhering to the policies. Another would be to send test phishing emails to record how many employees are still clicking into suspicious emails that are not related to work or the company at all. This test should not look like it came from the company or make the promise of any company compensation and be a dead link that leads to nowhere and just send analytics back to the proper department for analysis.