**STEP 1: SilverCorp - (GeldCorp Competitor)**

DATE: 5 October 2020

AUTHOR: G-Security (David Billings)

NO Private Phone Usage

PURPOSE

To Completely mitigate Internet and Network security risks due to private phone usage.

DESCRIPTION To protect against malicious cellphone malware such as keyloggers, ransomware, phishing techniques and other malware. Some examples of keyloggers are: <https://www.androidkeylogger.com/> and h[ttps://www.clevguard.com/android-parental-control/](https://www.clevguard.com/android-parental-control/) .

Some malware that employees would be trained about is <https://thehackernews.com/2020/04/android-banking-keylogger.html?m=1> and <https://www.avira.com/en/blog/mysterybot-the-android-malware-thats-keylogger-ransomware-and-trojan> , which is a keylogger, ransomware, and trojan All-In-One! Personal phones should not be used for checking work emails, Handling client support calls, Signing into work accounts from personal devices, or ANYTHING work related. Company phones will be issied to all personnel who need them. Ie. Brokers, Chairmen, etc. Cyber-Awareness training will be required with the use of any company device. Personal Devices include, but are not limited to: Android Cellphones/tables, Iphones, IPads, BlackBerry, etc.

ENFORCEMENT

Personal cellular phones will not be allowed on the work floor, inside cubicles or personal offices, inside lunch rooms, inside bathrooms, or anywhere past the Employee locker room. They must be kept locked inside your personal lockers, or left in your vehicles. Any personal cell phones found on the work floor will be seized by security and scanned for any malicious activity. If activity is found to be present, the device in question will be wiped. Personnel choosing to bring personal devices into the workspace will suffer the risk of losing all personal data on their personal devices as well as serious administrative actions.

MONITORING

Security will maintain constant patrols around the interior halls of the facility, occasionally stopping inside personal office spaces or cubicles to inspect for personal electronic devices. Security will not invade personal space unless there is good reasonable doubt. Invading of personal space does not mean looking inside desk drawers, as the desk and its contents belong to SilverCorp. Invasion of personal items being purses/backpacks/etc... Security may routinely call employees listed numbers with Human Resources and listen for ringing or vibrating anywhere in the facility.

**STEP 2: INVOLVE PEOPLE**

Chief Information Security Officer - This person’s role would be to coordinate between the CIO and security guards. They would handle most of the actual technical work, and scanning of devices.

Chief Information Officer - This person would be in charge Issuing company phones to employees who need them. Also as a backup list of infractions.

Chief Executive Officer - This person would need to be involved because it’s their head on a pike if clients’ personal information gets leaked. They are responsible for all employees beneath them, and making sure the other “Chief's” do their respective job.

Security Guard (captain?) - This role is very important because they will be doing the daily, random walk arounds the facility to see if anyone has or is using their personal devices.

All Employees - Must be informed of new policy changes, escpecially with the new confiscation of personal devies rule. It is primarily the employees responsibility to stop the use of these devices.

**STEP 3: TRAINING PLAN**

The only real training in this scenario would be what is allowed on the new company phones. Long story short, nothing but company related traffic would be allowed. Meaning you could call your clients, or have clients call you. You may call fellow co-workers/colleagues, but personal phone calls and/or text would be strictly prohibited. No checking of personal emails on company phones. If it doesn’t explicitly benefit the company, don’t dont it on a company phone. Company E-mails would be allowed on company devices.

This training will be held for all employees initially. Then it will rotate 50% of the staff every quarter, so that every employee gets this training bi-annually and the groups rotate. So you will have different partners/colleagues each time you attend this training scenario. Employees will cover topics such as malware, ransomware, keyloggers, backdoors, malicious E-mails, and be taught how to notice or look for suspicious activity both in people and on their electronic devices. This training would also cover all of the malicious software previously mentioned in STEP 1: The Description as well as ongoing and new threats that may arise.

The Chief Internet Security Officer (CISO) will be in charge of maintaining the active and new threat-list and presenting these new threats in detail to the employees at every meeting. This will ensure all employees are actively trained on the most current threats deemed appropriate by the CISO and other security staff.

Security guards will receive extra training on situational awareness, and suspicious behavior and/or activity. Security will also undergo a more in-depth in-house Cyber-Security training. This will allow security to have a full understanding of any situation that might arise from personal electronic device usage.

**STEP 4: OTHER SOLUTIONS**

One **Physical Alternative** to this policy would be having a Security Guard wave a metal detecting wand over every employee upon entrance. Storing their cell-phones at security until they leave; if they brought them through the check-point. This goail is **Preventative.** One definitive setback to this alternative would be how long it takes employees to get from their cars to their desks. It would also require a separate room for security to store confiscated belongings in bulk. However, this would totally mitigate all personal cell phone use within the facility.

A **Technical Preventative** measure could also be to totally disable all internal wifi networks and install cell phone signal jammers throughout the entire facility. Forcing employees to use land-lines and corporate internet for all communication done internally. One downside to this method would be that employees would not be able to communicate as easily with each other or the customer. The best part of this alternative though, is that every employee would have their own dedicated line and still have the proper cyber-training related to phishing and malware.