

UofT SCS

CYBERSECURITY BOOTCAMP

HOMEWORK - UNIT02 - GRC

Flavio Lopes

[**## GRC Homework: Assessing Security Culture**](#_wvunb47720lz) **3**

[**### Deliverables**](#_h7hhlxnnglzr) **4**

[**#### Deliverable 1: Measure and Set Goals**](#_8jnekxa7hf8z) **4**

[**#### Deliverable 2: Involve the Right People**](#_3bb6slgiwyr9) **5**

[**#### Deliverable 3: Training Plan**](#_cuthz5libytk) **6**

[**#### Deliverable 4: Other Solutions**](#_tb4k5b7u48dx) **7**

# ## GRC Homework: Assessing Security Culture

**User case:**

This week we learned about security culture and how to promote it within organizations.

It’s important that all employees are aware of common security risks and treat security seriously. The majority of cyberattacks aim to exploit human weaknesses with methods like phishing.

For this reason, people are most often the weakest link in an organization’s security defences.

For this unit’s homework, you will analyze the following security concern:

- Employees at SilverCorp are increasingly using their own personal devices for company work.

- Specifically, over half of all employees check their work email and communications via Slack on their personal mobile phones.

- Another 25% of employees are doing other work-related activities using work accounts and work-related applications on their personal phones.

- Allowing sensitive work information to be shared on employees’ personal devices has a number of security implications.

For this week's homework assignment, you will research these security risks and use the security culture framework to develop a plan to mitigate the concerns.

Below are the deliverables for this week's assignment.

# ### Deliverables

## #### Deliverable 1: Measure and Set Goals

***Answer the following questions:***

***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.*

The potential risks of BYOD

1. Data Leakage

Regardless of whether your employees need to access their corporate email or protected payroll information via mobile, data leakage is a possibility when personal devices come into play. Data can be lost or exposed when devices are misplaced or stolen, or if a personally-owned device has malware on it. While cloud technology has mitigated most data loss due to device damage, security barriers and backups are crucial to a healthy BYOD program.

2. Sketchy Apps

Not all personal apps are what they appear to be, or have any business being on our end-users' mobile devices. Back in July, you may remember the Pokemon Go craze and the large quantity of fake and malicious apps. TechCrunch reports that some of the confirmed malicious apps included titles such as "Pokémon Go Ultimate," "Guide & Cheats for Pokémon GO,” and “Install Pokémongo," in order to appeal to fans of the game.

In some cases, malicious apps have the potential to take control over the user's mobile device. This can result in surveillance, unexpected data or call charges, or loss of personal and work information.

3. A Lack of Management

With any mobile device, employee or company-owned, there are risks associated with a loss of control. When an endpoint walks out of your company's building, it can be difficult to control whether it's used on questionable free wireless connections or whether it will be misplaced and stolen.

4. Device Infection

The vast majority of users with an infected smartphone don't know their device is carrying malware. Even more concerning, feelings of "app fatigue," or excess exposure to mobile content, can make users care less about mobile security. They may not read the terms of service on new apps or think twice before granting excessive permissions when downloading new content.

Outdated mobile operating systems can be a major risk factor, with some of the most vicious forms of malware primarily affecting outdated OSs. Even new OSs have vulnerabilities, so it's also crucial to use file integrity monitoring to immediately detect and act on device infection.

5. Poor Policies

It may be possible to attempt a BYOD program without effective security policies in place, but it's certainly risky. If your organization is required to comply with PCI DSS, HIPAA, or any other regulatory requirements, effective policy is necessary to avoid fines.

6. Mixing Personal and Business Use

With BYOD, mixing business and personal use is inevitable. You can't control whether your employees decide to shop online at compromised websites or whether they will misplace a device. While you can educate heavily on security best practices, you can't guarantee that your employees won't loan their device to a friend or use public wireless connections to save data.

7. Inability to Control Devices

What if an employee leaves the organization or loses their mobile device? In many BYOD programs, the majority of the security stress comes from a lack of control around devices. Employees are not always careful, and disgruntled staff can do a lot of damage with too much access.

For the potential attacks we can mention:

Adware, fake apps and AD Frauds

Targeted attacks

Malware

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

First of all, it’s important to set clear security policies and educate the users, after this education we should expect the following behaviour:

Do not install software from unknown sources.

Do not open an email(s), click on a link or open files received from unknown sources.

Use your common sense. If the website looks unsafe, don't open it.

Check the URL carefully. Phishers will set up a web page almost identical to the original one. They use this tactic to stolen personal data.

All employees must promptly report the theft or loss of their own devices.

*3. What methods would you use to measure how often employees are currently \_not\_ behaving according to the preferred behaviour?*

The following tests can be conducted to test the adherence to the security policy and the preferred behaviour.

**Administer quizzes.** The folks who host security awareness training should administer multiple-choice quizzes during training and a few times each year at random. Post a Web-based quiz and vary the questions so employees don't get used to a pattern or share answers in order to get it over with as quickly as possible.

**Perform random work area checks.** Employees can become desensitized or complacent with the information around them. Check employee desk security for documents and sticky notes that contain confidential information. Are they out in the open so anyone walking by can view or take them? See if filing cabinets are locked and if document storage boxes are left in unlocked work areas. Also check whether employees' computers are still logged on, without password protection, when they're away from their desk.

**Become a white hat social engineer.** Appoint a staff member who isn't well known in the organization (or hire a consultant) to call employees or stop by their desks, requesting confidential information such as logon credentials or information in a non-public document. The social engineer should have a "pertinent" story ready as to why he or she needs the information.

**Simulate phishing email attacks.** A phishing email contains links to malicious websites or payload-filled attachments. The email is designed to look legitimate, which throws off the typical user. One of the best ways to find out if employees are mindful of phishing emails is to send some to their inboxes. Your test emails should contain some clues that they are not from the purported sender (for post-testing educational purposes) and contain links that go to a safe website. The site could simply be a page that says, "Security awareness training — phishing test in progress." Security technicians can gather IP addresses of visitors to the page to monitor which employees visited the site and therefore clicked the link.

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

Once the policies are created, approved, part of the user education and part of a continuous assessment procedure; the company should expect the user to behave under the security policy in-place.

## #### Deliverable 2: Involve the Right People

*Now that you have a goal in mind, who needs to be involved?*

Depending on the size of our corporation the following professionals should be part of the decisions:

**CEO- Chief Executive Officer**

The CEO is the main responsible for managing a company and, therefore, is ultimately responsible for the results and performance of a company.

**CIO- Chief Information Officer**

The Director of Information Technology is responsible for aligning information technologies with the company´s strategy. This person focuses on improving the efficiency of processes and on the analysis of new technologies.

**CSO- Chief Security Officer**

CSOs are in charge of Corporate Security. Their main responsibility is to guarantee the physical and technical security, and for that, they must identify what assets they need and how to protect them.

**CISO- Chief Information Security Officer**

This role is one of the most recently created organizational roles. The main role of CISOs is to monitor and analyze the risks that a company faces in order to guarantee data and information protection.

**CTO- Chief Technology Officer**

CTOs are responsible for information technology. This role is quite similar to that of a CIO, but the approach, in this case, is more technical.

**CDO- Chief Data Officer**

It is the role that has probably been created most recently but it is having a great projection. According to Gartner, in 2014 only 400 of the main organizations had a CDO, but it is expected that by 2019, 90% will have this figure.

The CDO is the person in charge of the data strategy (protection & privacy).

**HR Director**

HR directors are responsible for the smooth and profitable operation of a company's human resources department. Typically, they supervise and provide consultation to management on strategic staffing plans, compensation, benefits, training and development, budget, and labour relations.

**IT Security Department** as a whole has also other professional specialists usually focused on their own areas of expertise, for example, **Security Incident Manager, Penetration Tester, Cyber Risk and Compliance Specialist, Cyber Security Strategist, Cloud Security Specialist, DevSecOps Specialist,** etc..

## #### Deliverable 3: Training Plan

*Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:*

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

As part of the training process, we will implement:

In-person training for all new employees as part of their on-boarding process.

On-line training every 6 months for all employees.

The continuous assessment process will dictate any change in the training procedure or interval.

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

All the essential topics in the training are listed below

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

After the training, a questionary will be required to be answered by the employee with a pass mark of 100%.

*This portion will require additional outside research on the topic so that you can layout a clear and thorough training agenda.*

**1: Define what BYOD means for the organization**

BYOD training should start with an introduction explaining what BYOD brings to the organization. This leadoff to the training should sell the initiative to your users while relating the effort to what it offers the overall business and your customers.

This introduction is also the time to clear up any misconceptions of BYOD at a high level. Unfortunately, a lot has been written about the downsides of BYOD. The training needs to tell the benefits BYOD is bringing to your organization.

**2: Cover the process of onboarding BYOD devices**

Onboarding devices into a BYOD program can be done in conjunction with BYOD training. Even if you choose to onboard devices at another time, users need to know exactly what software their organization is installing on their personal device(s). This part of the training also addresses:

Supported devices

Supported mobile operating systems

Supported apps, such as mobile office suites and productivity apps

Debrief And Defend: Choosing Linux instead of Windows Vista

Microsoft advocates Windows Vista as the operating system of choice for desktops. But there are plenty of adherents to the Linux operating system who say that it's a better choice. Is it really? The Choosing Linux instead of Windows Vista presentation...

Tools & Templates provided by TechRepublic Premium

Likewise, the training needs to cover what happens to corporate network access on a BYOD device when the employee leaves the organization.

**3: Explain expense reimbursements and/or stipends**

ADVERTISING

I put expense reimbursements high up on the training list because corporate usage of personal mobile devices means reimbursement for minutes and data usage that a user with a BYOD device might incur. While service management and expense reporting policies should be clearly documented, BYOD training is the time to open up the discussion about the expense policies.

If your organization is choosing to offer users a stipend for BYOD expenses, training is a good time to cover the stipend in detail. You can even have attendees apply for their stipend while they are attending the training session.

**4: Define BYOD device security policies**

User security across personal laptops and other mobile devices might run the gamut, but using the devices for BYOD means the organization needs to set security policies for them with the documentation to back up the security decisions.

When you include BYOD device security policies as part of BYOD training, it's important to cover the following topics:

BYOD device password policies

Corporate WiFi network security

Hotel/public Wi-Fi security

BYOD device loss or theft policies

**5: Review data ownership policies**

Corporate data ownership policies should be in place when you launch a BYOD initiative. When corporate and personal data intermingle on a personal device, BYOD training should cover what the user can expect for corporate control over the data residing in their data. The training over data ownership policies could extend to the following:

Corporate vs. personal email

Social network access and account ownership

Business vs. personal contacts

Corporate data residing on the mobile device

**6: Define what MDM is (and what MDM isn't)**

Mobile device management (MDM) provides security, management, and provisioning tools for BYOD devices that exist in the corporate enterprise. Introducing MDM onto a personal device is also the one element where corporate security and personal property interact and can lead to some big misconceptions.

While the overall BYOD policy should define the role of MDM, you can use time during the BYOD training to reinforce MDM understanding, including:

Break down a typical BYOD device and show how MDM affects the device features and MDM security.

Describe MDM features and how they benefit the BYOD user.

**7: Teach how to use mobile office suites on corporate documents**

Tablet users might be interested in using mobile office suites, such as Quickoffice Pro HD and DocsToGo Current. Next-generation iPads and Android tablets are packing in the horsepower, with the mobile office apps adding new features. However, there are still questions to address during BYOD training, including:

Document security, such as policies set to prevent BYOD devices from having editing access to certain corporate documents.

Recommended mobile office app(s) based upon a test of accessing a selection of your organization's documents.

Using a SharePoint iPad client such as Harmon.ie or one of the other apps I profiled in Top apps for accessing SharePoint to access documents.

8: Define the responsibilities of BYOD device users

Responsibilities for BYOD users should be defined in the policy guidebook, but BYOD training is the time to address the more technical responsibilities -- including logging in to the network to receive software, security, and app updates.

**9: Teach how to access corporate resources from BYOD devices**

If a BYOD initiative is prompting an influx of new mobile users into your organization, training should encompass how to use mobile devices to access the standard corporate enterprise resources that the BYOD users have permission to access, including:

Virtual private network (VPN)

Corporate email

Salesforce automation tools

Customer relationship management (CRM) system

Even if some of these systems are already familiar to your users, putting them in the training and in the context of BYOD is what's important.

**10: Teach about technical support and escalation paths**

The lines of support for BYOD devices may not always be clear when you first embark on a BYOD initiative. Tech support responsibilities most certainly have their place in the overall corporate BYOD policy, but they also need a spot in BYOD training to address:

Escalation paths for BYOD device issues that happen during the course of business.

Escalation paths for lost or stolen BYOD devices when the event occurs during the course of business.

Level of support that the organization offers per device type.

One other suggestion is to include any self-help sites for device users, especially those who travel frequently.

## #### Deliverable 4: Other Solutions

*Training alone often isn't the entire solution to a security concern.*

*- Indicate at least two other potential solutions. For each one, indicate the following:*

Two controls for BYOD mobile devices*:*

1. Immediate notification for lost and stolen devices
2. Mandatory encryption in any device

*\* What type of control is it? Administrative, technical, or physical?*

1. For number 1 above is administrative
2. For number 2 above is technical

*\* What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?*

1. Compensating
2. Preventive

*\* What is one advantage of each solution?*

1. Once a device is reported, IT should terminate the device’s access to the network and any apps accessing company data. IT can also remotely wipe company data from the phone, if necessary.
2. Encryption an extra layer of security to the data in the mobile device in the case of a lost or stolen device.

*\* What is one disadvantage of each solution?*

1. Since phones are often lost outside of business hours, it is essential to have a contact person and procedure 24 hours a day, seven days a week.
2. An old device can experience slowness after encryption

## #### Refferences:

[The 7 Scariest BYOD Security Risks (and How to Mitigate Them!)](https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate)

[Review, Refocus, and Recalibrate: The 2019 Mobile Threat Landscape - Security Roundup](https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/review-refocus-and-recalibrate-the-2019-mobile-threat-landscape)

[CEO, CIO, CSO, CISO, CTO, CDO Who´s Who in Cybersecurity?](https://randed.com/cybersecurity-roles/?lang=en)

[10 essential elements of BYOD training](https://www.techrepublic.com/blog/10-things/10-essential-elements-of-byod-training/)