Assessing Security Culture

By Anna Petryk

Deliverable #1
Measure and Set Goals

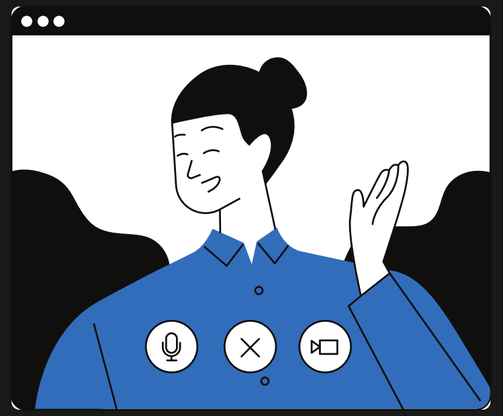
Usage of personal devices for work-related activities is a primary concern include potential attacks that can influence Confidentiality, Integrity and Availability of the company.

- Employees could tweet negatively about your company or colleagues.
- Keeping a copy of confidential work documents in case they need them in their next jobs.
- Taking a copy of work software home for use on their personal computers.

POTENTIAL ATTACKS

EMPLOYEE PREFERRED BEHAVIOR

1. Use only work-provided devices for work-related activities that are properly administered by the company.



2. Do not use Slack and work email on personal devices that are properly administered by the SilverCorp.

3. Do not use work accounts and worked related applications on personal devices that are properly administered by the company.

4. Do not store confidential and work-related sensitive data that are properly administered by the SilverCorp.

PREFERRED BEHAVIOR MEASUREMENT

1. Monitor the connections to the email server.
2. Determine Device ID if the devices is work-issued.
3. Implement Device Policies to the the devices to monitor applications and usage. Make sure only work-related applications were installed and used.

Goals

Security Culture

SilverCorp

1

Issue mobile devices and train employees how to use it.

2

Install Mobile Device Management software and assign the team to administer them.

3

Sensitive work information NOT to be shared on personal devices.

4

Decrease usage of personal devices.

5

Improve Security Culture.

Deliverable #2
Involve the Right People

CEO

Support IT and HR Team with enforcement of the policies in order to mitigate risks that are related to Confidentiality, Integrity and Availability of the company.

CIO

Create and enforce IT Policy to issue devices to all employees that require that and administer application and data being stored on that devices.

HR

Director

Issue a communication to the employees of the company reminding personal device policy and coordinate with IT to issue work devices to the employees, which can be administered by IT department.

Deliverable #3
Training Plan

1. Perform Annual In-Person Training. Measure the results and based on that decide if another In-Person Training required.
2. Send Internal communication with updates or additional information on weekly basis.
3. Mandatory Interactive online hands-on training to make sure all employees agree and consent to IT security policies.

Topics to discuss during the training:

- What is Cybersecurity and why it's important
- Mobile Device Management Policy and how to use work-issued devices. Usage and Applications
- VPN and Web Protection
- 2FA and Passwords
- Phishing emails
- Data Security and Privacy

Measurement

- Verify 100% of employees completed mandatory online training.
- Send Read Receipts with internal communication to measure % of employees have read the emails.
- Based on the results from periodic security review, measure % of security improvements following the annual In-Person training.

Deliverable #4
Other Solutions

1. Create and Deploy Policies to enforce Administrative Security Controls
Detective

- 2 Factor Authentication Policy to ensure the right person uses the right device.
- Password Management Policy for all employees to change password monthly and use password protected access controls.

+ More controls around passwords and login will create less vulnerabilities within human factor
- Employees can forget their new password and lock themselves out. Loss of registered 2FA device or change a phone number

2. Mobile Device Management (MDM) Software is crucial to monitor devices. It helps to implement security settings and manage the location of devices. (Physical and Technical Control)
Preventive

+ Allows to limit access to work-related activities within work hours and physical location of the building.
- Resource requirement to administrate the devices.