### Deliverable 1: Measure and Set Goals

While there are plenty of potential security risks of allowing employees to access work information on their personal devices, there are also numerous benefits. This work policy will be referred to as BYOD culture within the rest of this report. BYOD culture's potential risks include local exposure, data leakage or loss, public exposure, and malicious apps. Local exposure is one of the inherent downsides of BYOD because you have a loss of control and visibility of enterprise data which is being transmitted, stored, and processed on personal devices. Potential data leakage or disclosures can occur if accessed on unsecured devices. Physical loss or theft of a device could cause a loss or compromise of sensitive data. Public exposure occurs when personal devices are accessed through public wifi hotspots. Malicious applications can sniff, modify, or steal inter-application messages and compromise trusted applications on personal devices. The view on mobile devices also poses another risk because of the simplified views shown. For example, the headers on emails are shortened to only show the Name as opposed to a full email address. This makes it more difficult to identify phishing emails that have changed the header of the email address to appear to come from a trusted source. These emails may be after data or have malicious download attachments that install malware on their device. Data leakage can also occur from ex-employees having company data stored on their personal device after termination.

We need to have the employees engage in the following behavior: All employees need to verify that emails come from trusted sources by viewing the full email address before clicking on any links or downloading any attachments. All employees should have antivirus/malware security protection applications installed on their devices. All employees should have activated phone access security through biometrics or a secure password.

In order to measure the employees' current behavior, and that after training, a survey should be created to analyze current employees' actions associated with accessing emails on their personal devices, and actions associated with clicking links, downloading attachments, installing applications and current security settings on their personal devices.

Our goal through this mitigation is to decrease the click-through rates from untrusted sources to less than 5%. We want to decrease downloading attachment from untrusted sources to under 5% as well. We also want to increase employees' overall security knowledge and compliance with security standards to over 97%.

### Deliverable 2: Involve the Right People

It is important to make sure to involve the right people in this process. For this project, we will involve the CFO, CIO, CISO, HR Department, and IT Department.

The **CFO**, Chief Financial Officer, would provide the role of approval and be involved with the budget. They would assist in the creation of the budget and give the final approval on all financial expenditures for this project. They would be the one to analyze the ROI for IT support and licenses for security software.

The **CIO**, Chief Information Officer, would perform the role of enforcing and monitoring the approved standards. They would also be in charge of managing the IT department's deployment of support.

The **CISO**, Chief Information Security Officer, would perform the role of creating the standards. They would also be in charge of creating the surveys for tracking employee behavior and monitoring the progress through these surveys. They would also be in charge of testing the system to ensure the standards incorporated are sufficient to mitigate the risks.

The **HR Department**, Human Resources, would perform the role of distributing this information to all employees. They would be in charge of making sure that the employees take the entry survey, complete security training, and distribute the follow-up surveys for monitoring progress.

The **IT Department**, Information Technology, would be responsible for setting up the security settings established by the new policy. They would also be in charge of verifying or installing antivirus/malware protection applications on the employee's personal devices. They would also provide on-going support to employees with all security technology and follow-up questions.

### Deliverable 3: Training Plan

It is important to make sure all employees get sufficient training on all aspects of security in order for them to safely use their personal devices. Initial training will be provided in-person so that the IT staff can assist everyone in setting up their phones with the proper security settings. Additional training for employees who require additional training to increase their security standards will be offered online. In-person one-on-one support will be available during regular work hours for all employees. Training will be provided monthly to ensure that new employees have access to training in a timely manner. The main topics that will be covered are phishing and social engineering; access, passwords, and connections; device security; and physical security.

Phishing and social engineering and how to protect against it. Social engineering is based upon disguising themselves as credible sources. Therefore it is important to make sure employees are aware of red flags to look for to avoid phishing emails, phishing SMS texts, and phishing voicemails. The key is recognizing that something is off about the information that is being requested. This is particularly important with mobile devices since the screens are smaller and the views are limited, making it more difficult to recognize missing aspects of credible sites and email accounts. Best practices include not clicking on links or attachments and to inform the IT team.

Access, passwords, and connections and best practices. Each employee needs to be informed of the access they have, including which applications they can and can not access. Best practices on strong passwords should be taught and enforced. Passwords should also be changed every six months. Basic information about the risks involved in accessing data through public networks should be thoroughly covered. Informing employees that certain networks won't support the encryption the data has in transit from the organization.

Device security and assisted setup. For this portion of the training, it will be important to have employees attempt to set up the security on their phones. This show and tell method will help them learn the reason behind the requirements. It can also assure they are less likely to feel that their privacy is being invaded by this setup process.

Physical security is still important too. This portion of the training will emphasize the importance that their devices always be in their possession and are never left unattended. This portion will also include a brief overview of policies for getting rid of devices that were used for company use.

After employees have completed training, they will be given a follow-up survey to measure the employee's improvement in knowledge and practice standards. This measure will also be used to determine requirement of additional training for the lowest-performing employees.

### Deliverable 4: Other Solutions

In order to get a fully comprehensive plan to mitigate the risks sufficiently, there are other solutions that need to be incorporated. Data should be encrypted so that it is safe when in transit to these mobile devices. This will protect the data when accessed in less secured networks. This is a technical control. The goal is preventative and deterrent. An advantage of this solution is that data is protected. A disadvantage to this solution is that it can slow down the process of obtaining the data, which could limit employees' productivity.

The IT department should review all employees' devices in order to verify that security is sufficient. This review should ensure that passwords or biometrics are correctly enabled; sufficient antivirus/malware applications are installed or install applications provided by the organization; and that remote wipe is enabled for the organization to initiate in the event of loss or theft. This control is both physical and technical. The goal is both preventative and corrective. An advantage is that data is secured and there is protection against loss and theft. A disadvantage is that employees may feel that their privacy is invaded, or may feel that they are being monitored when off-the-clock.

The HR department should create an off-boarding policy and ensure it is enforced in order to make sure that all company data is removed from personal devices before termination. This control is administrative. The goal is preventative. An advantage of this solution is to limit the risks associated with corporate espionage from disgruntled ex-employees having access to company data. A disadvantage would be the hours required by the HR department to enforce this policy.

### Sources

Hoelscher, Penny (Nov 5, 2017) *BYOD security: What are the risks and how can they be mitigated?* Retrieved from https://www.comparitech.com/blog/information-security/byod-security-risks/.

Lord, Nate (Feb 27, 2018) *The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits.* Retrieved from https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating.

The Security Culture Framework Community site. Retrieved from https://securitycultureframework.net/.

Teplow, Lily (Aug 5, 2019) *The Basics of Cyber Security Training for End-Users*. Retrieved from https://www.continuum.net/blog/the-basics-of-cyber-security-training-for-end-users.

Snyder, Joel (Jun 27, 2018) *4 Ways to Improve Mobile Security Training for Employees*. Retrieved from https://insights.samsung.com/2018/06/27/4-ways-to-improve-mobile-security-training-for-employees/.