Steps for Staging Your Town Hall

1. **Recruit the right people to form the planning committee**
    a. Ensure that management, the HR and IT departments are present for planning, and are aligned on the objectives and expectations of this Town Hall. Representation from these functions is important because these departments not only lead the corporate agenda for cybersecurity, but also provide a balanced perspective for more effective engagement.
    b. Identify the most appropriate speaker to lead and moderate a Town Hall on the company's commitment to cybersecurity. Consider who would be the best candidate to make cybersecurity seem accessible to the average employee.
    c. Understand your employees' attitudes towards and understanding of cybersecurity, so that you can decide on what is the best tone and style to use for your Town Hall.
    d. Hold a pre-meeting to discuss potential questions or problems and how to most effectively respond to various issues. Use this time to also ensure everyone is comfortable with the agenda and the presentation style or format of discussion.

2. **Choose an appropriate date and time.**
    a. This refers to when most employees will be around.
    b. Block half an hour for the town hall by sending out a calendar invite and alerting department heads to let employees make the necessary arrangements beforehand.
    c. Try to avoid common busy periods and pick timings when employees tend to be at their most focused.
    d. Take care to avoid scheduling the Town Hall in the middle of the afternoon, or right before the standard knock-off time.

3. **Prepare materials to distribute onsite if necessary.**

   These materials will help supplement the agenda for your town hall. These could include your company's own cybersecurity policy or an overview of your company's expected roll-out of the Kit.

4. **Review and refine the town hall agenda.**

   We have prepared a sample agenda in the next section for you to adapt according to your company's needs. Consider what your company is prepared to talk about, what your corporate culture regarding cybersecurity is like, and also any possible issues your employees might bring up.

5. **Prepare the venue.**

   a. Ensure there is enough space for employees to sit or stand.
   b. Ensure all lights and AV equipment are working.
   c. Ensure that involved parties know where to stand.
   d. Consider preparing extra microphones so employees can speak up and ask questions that can be heard clearly by the Town Hall moderators, speakers and the rest of the audience.

6. **Hold a debrief meeting.**

   This allows the planning committee to come together and discuss how to proceed with executing the rest of Level 2 of the Employee Cyber-readiness Kit. The messaging, tonality, level of employee guidance and timing details roll-outs should be reviewed in accordance to the corporate culture and needs of employees.

   Post Town Hall debrief meeting agenda should touch on the following:

   a. Learnings from the Town Hall.
   b. Feedback from employees and how to follow up on it
   c. Next steps in terms of executing the Employee Cyber-readiness Kit

Proposed Agenda (30 min)

1. **Introduction (2 min)**
    a. Welcome employees and thank them for attending.
    b. Be clear about the length of the meeting and the items on the agenda.

2. **Explain the purpose of the Town Hall (8 min)**
    a. Remind attendees of the company's commitment to cybersecurity.
    b. Share examples of why cybersecurity is important at the workplace.
        i. According to the 2018 IBM X-Force Threat Intelligence Index, human error was found to be responsible for two-thirds of compromised records. Some of the most common scenarios involve basic misjudgement in the form of storing intellectual property on insecure personal devices, falling for phishing emails, erroneous permission-level attribution on cloud services, and exposed sensitive data through weak or non-existent authentication.
        ii. Verizon's 2017 Data Breach Investigations Report found that social attacks, like phishing, were utilized in 43% of all breaches, leading to events like software installations and influencing disclosure of sensitive data.
        iii. A state of the industry report in 2018 by Shred-It found that 26 percent of staff admitted to bad security behaviour at work, for example leaving their computers unlocked and unattended. The same report found that nearly half of the C-Suites interviewed have had employees who have lost or had their company devices, like phones or computers, stolen.

3. **Update on the company's agenda on cybersecurity (5 min)**
    a. Share the overview of cybersecurity policies on infrastructure, hardware and software that the company has already undertaken, and however comprehensive these policies are, that they do not address the 'wild card' of human error.

4. **Share how the company has been working on employee education on cybersecurity (5 min)**
    a. Point out how, to address this 'wild card', the company has been working on educating employees on how to keep safe themselves and one another safe online, through assets such as the Top Tips and electronic direct mailers.

5. **Share how the company will be taking next steps to up the ante on employee education on cybersecurity (5 min)**
    a. Share how there will be more ways to engage on cybersecurity coming up in the next few months
    b. Introduce each of the elements, their objectives and how employees can get involved
    c. Encourage employees to come up with their own suggestions on how to up the ante

6. **Question and answer session (5 min)**
    a. Invite employees to share concerns and questions

Tips for a Successful Town Hall

1. **Be prepared.**
   Have thoughtful arguments, specific points, good data, and a clear agenda. Ensure that everybody in the planning committee is on board and aligned on what is required of them.
2. **Commit to real dialogue.**
   A Town Hall meeting is a place for a conversation, not a monologue. It is important to engage the employees to encourage them to take ownership of the topic.
3. **Ensure you follow up.**
   You might not have been able to address all questions and concerns that surfaced during Q&A. Consider creating an e-mail address for employees to contact via e-mail, or an online feedback form, with the questions and concerns going to the person assigned the charge of carrying this out.