Eat Hackers for Lunch Campaign: Operational Plan

Matthew Schroeder
Liv Erickson
Matt Sievers
Alexander "RoRo" Romero

CONTENTS

Big Security for Small Business
http://www.smallbiz-bigsec.org

Document Purpose and Target Audience

The "Big Security for Small Businesses" website features the "Eat Hackers for Lunch" cybersecurity campaign, a set of recommendations and infographics that organizations can use to improve their cybersecurity awareness. This document reviews how we, the authors of the campaign, recommend using the Eat Hackers for Lunch materials in an interactive campaign.

We recognize that different organizations will have their own needs and ideas, and so we encourage organizations to use their own best judgment in tailoring these materials for their use.

The target audience for this document includes:

1. Cybersecurity-focused public/private partnerships that have experience performing awareness and outreach campaigns;
2. State, local, tribal, and territorial (SLTT) government agencies responsible for providing cybersecurity and/or evaluating the cybersecurity of third-party vendors;
3. Advocacy groups interested in helping small businesses better secure their digital resources.

Campaign Details

Campaign Background and Purpose

The "Eat Hackers for Lunch" campaign was created as part of an Aspen Tech Policy Hub project to bring "big security to small businesses." The overall goal of the campaign is to get small businesses to incrementally improve their cybersecurity through simple, bite-sized cybersecurity activities that can be completed over a series of lunch breaks.

The campaign is currently presented through the Aspen Tech Policy Hub project website in a self-guided format. It consists of five activities that the Aspen Tech Policy Hub project team (hereafter referred to as 'the project team') deemed to have the highest cybersecurity return on investment (ROI) based on the level of effort required. Once the employees of a small business perform these activities, their level of security will improve.

Design Principles/Guidelines

We describe below a proposal for how the campaign can be implemented. To maintain the intent of the campaign, each activity/module should be designed so that it:

1. Could reasonably be performed by someone with some IT background, but no significant information security background.
2. Provides at least some positive cybersecurity impact at completion, as opposed to being only an intermediate step toward effectiveness.
3. Take no more than 5-7 hours of work (about one week's worth of lunch breaks); and
4. Integrates lunch theme/food-based characters to make the modules more-interesting and relevant to users completing the activities during lunch.

Vision and Ideas for the Campaign in the Future

The project team designed the campaign so that other organizations can build upon it in the future. Ideally, the campaign would gain sponsorship and support to make it more widely used and targeted to a broader base of users. Other potential areas of growth for the campaign include:

1. Evolving to include activity roadmaps that allow small businesses at all levels of cybersecurity maturity to "level up";
2. Incorporating support and/or "office hours" with local officials or volunteers to help small businesses that have questions or challenges with any of the activities; and
3. Expanding upon food-based characters and providing videos and even VR experiences to attract users and keep them engaged.

Pilot Campaign

The next step is to pilot the campaign with a limited group of small businesses. The goal for participants is to have implemented — or at least developed a plan to implement — all the activities in the "Eat Hackers for Lunch" campaign.

Selecting Instructors

The pilot instructor should have experience providing cybersecurity training to businesses. Ideally, the instructor's experience will include working with small- or medium-sized businesses and implementing the security tools and services included in the campaign recommendations.

Optional resources: additional cybersecurity subject-matter experts, possibly volunteers, could help supplement the instruction in case of a high volume of

questions and requests for help from participants.

Selecting Participants

To maximize the value of the pilot, small businesses participating should not have completed most, if not all the activities covered in the "Eat Hackers for Lunch" campaign. Additionally, the group of small businesses in the pilot would ideally represent a mix of industries.

If the instructor does not have additional subject-matter expert support, it is recommended that between 3-5 small businesses participate.

Pilot participants from small businesses would need to commit the following:

1. One representative, preferably the person within the company most directly involved with IT or information security;
2. Between 5-7 hours a week for two weeks to attend training sessions, perform security activities, and provide feedback;
3. Participation in the daily lunchtime meetings;
    a. Lunchtime meetings should be one hour long
    b. No more than two topics should be covered per lunch session
4. Willingness to try to implement recommended security activities; and
5. Willingness to provide feedback and recommendations during and following the pilot.

Estimated Timeline

The pilot should only take around two weeks since it should focus mainly on deploying the content within the series.

Implementation of Pilot

The pilot lead should create a roadmap for participants that incorporates the following materials:

1. Lightweight Assessment of Security Risk (LASER)
2. 'Eat Hackers for Lunch' Campaign Materials

Suggested Sessions

The following are suggested sessions for the pilot to cover the 'Eat Hackers for Lunch' campaign and provide support to participants.

Session Title	Day	Description	Duration
Week 1			
Kickoff	Monday	Explain program to participants, provide materials and directions, answer questions	1 hour
Security Session 1	Tuesday	Secure your Network Password Protection	1 hour
Implementation Day	Wednesday	During lunch, work on plans to implement learnings from Session 1; instructor hosts ad-hoc office hours and responds to email questions	1 - 2 hours
Security Session 2	Wednesday	Two-Factor Authentication Updating Applications	1 hour
Week 1 Office Hours	Friday	Attend office hours with instructor to get questions answered and discuss recommendations	1 - 2 hours
Week 2			
Security Session 3	Monday	Back Up our Data Group discussion on progress, challenges, opportunities, etc.	1 hour
Implementation Day	Tuesday	During lunch, work on plans to implement learnings; instructor hosts ad-hoc office hours and responds to email questions	1 - 2 hours
Week 2 Office Hours	Wednesday	Attend office hours with instructor to get questions answered and discuss recommendations	1 hour
Final Implementation Day	Thursday	Finalize security plans and implementations, identify next steps; instructor hosts ad-hoc office hours and responds to email questions	1-2 hours
Conclusion of Program	Friday	Gather participant thoughts and recommendations on the overall campaign	1 hour

Session Type	Homework
Kickoff	Review course materials, share and discuss with co-workers, start identifying what security capabilities your business does and does not have
Security Sessions	Identify solutions related to a Security Session topic that may work at your business, and start creating a plan for implementation
Office Hours	Implement learnings from office hours

General Session Structure

We propose that the training portion of the three Security Sessions should run as follows:

1. The instructor:
    a. Provides explanation of why the security activity and topic are important
    b. Demonstrates or describes real-world attacks that occurred because the security activities related to the session's security topic were not applied
    c. Demonstrates or describes how the security activities would have stopped the attack
2. Each participating company discusses what solutions, if any, it uses to implement the security activity and mitigate attacks
    a. Solutions may include people, processes, and tools used to implement security activities
3. Instructor walks through available solutions and best practices that other companies have implemented
    a. Demonstration of how to use different options
4. Q&A

Post-Pilot Steps

After the pilot is complete, the pilot lead should work with training stakeholders and partners to review feedback and share observations, with a goal to:

1. Determine the effectiveness of campaign materials and activities
2. Identify what factors contributed to the effectiveness
3. Compare preferences and needs across small businesses of different industries and cybersecurity capabilities; and
4. Develop a plan to update the campaign, based on lessons learned