Kendall Square
The Future Lives Here

Future of (how we) Work

October 2022 High Level Meeting Takeaways
Topic: Cybersecurity

Meeting & Agenda Overview
The hybrid work model paradigm comes with its own set of cybersecurity issues, which result from employees' use of a mix of business and personal devices from their homes, offices, and other locations, resulting in a hazy network perimeter. Therefore, it is important for companies and individuals to alter their cybersecurity plans to keep hazardous cyber threats at bay to account for these risks. KSA's October Future of (how we) Work virtual meeting featured Neil Jones, Director of CyberSecurity Evangelism at Egnyte.

Participants were welcomed into the virtual meeting by Caleb Hurst-Hiller, VP of Community Learning, and invited to share their names, company affiliations and ways they were currently keeping their digital privacy protected. Neil Jones then proceeded with his presentation on how to ensure personal and professional digital information is secure from hackers, malware, and phishing.

Presentation Takeaways:

- Colonial Pipeline made headlines in 2021 when hackers gained access to the company's data and took down the largest fuel pipeline in the U.S. and led to shortages across the east coast. The hack was the result of a single compromised password. Cyber attacks are becoming more and more commonplace as all of our personal and professional data are housed online. It is of the utmost importance to protect your and your company's data and privacy.
- Things to be mindful of to protect your company's data:
    - If you are a senior leader or part of your company's technology department, understand your staff's current IT needs and challenges. "Shadow IT" happens when formal IT infrastructure does not address staff's needs and a second informal IT infrastructure is created that operates concurrently as the formal structure. "Shadow IT" presents additional weak points in a company's privacy.
    - Be mindful of what information you share with colleagues and adopt a "need to know only" mentality. Employees should only be given access to the specific data systems that they need for their jobs or for a specific task.
- Things to be mindful of to protect your personal data:
    - Place an expiration date on file access if the information is particularly sensitive.
        - How to place an expiration date when sharing files using Google products.
        - How to place an expiration date when sharing files using Microsoft products.

    - Be mindful of the information you share in public and online spaces. For example, some stores will ask you for your phone number when you check out. Although it may seem innocent enough, your phone number is an important piece of personal data that can be used for nefarious purposes when hackers get ahold of it.

View Neil's presentation for additional information and cybersecurity tips.

Resources Shared:

- 5 Cybersecurity Trends Impacting Mid-Sized Organizations in 2022
- Cybersecurity for Small Businesses
- How to place an expiration date when sharing files using Google products
- How to place an expiration date when sharing files using Microsoft products
- I Shared My Phone Number. I Learned I Shouldn't Have
- How to Decline Giving Your Personal Information at Retail Stores