SPRING/SUMMER 2020 $25

The NOW WHAT? *Issue*

A new remote-work reality will mean long-term changes for how M&E gets business done. Welcome to Hollywood's new normal. *P. 15*

M AND E JOURNAL
Media & Entertainment
Strategies. Solutions.

published by
MESA
Media & Entertainment Services Alliance

5 Must-Haves for Microsoft Teams Adoption and Data Security

Negligent insiders can unintentionally pose a risk equal to that of bad actors

By David Salter, Director, Technology Solutions, LiveTiles

Abstract: As hackers grow increasingly bold — and successful — in their attacks, three recent trends dominate the M&E industry's cybersecurity landscape. First, content protection has emerged as a top issue with new security threats and increasing complexity in the production process. Second, new cloud tools increase productivity but can complicate security. Third, general cyber hygiene is playing a larger role as malware and ransomware attacks make the news.

Microsoft Teams adoption recently hit a new high with 44 million daily active users, spiking a whopping 37 percent in just one week due to the surge of employees working from home. Now more than ever, Microsoft Teams is facilitating group communication and productivity as employees across the globe transition to work from home in the face of a global crisis.

However, even in the best of times Teams can present governance and security challenges for organizations — especially for those who are fast-tracking deployment to support remote work. When Teams is not managed properly it can lead to issues that damage the business value it delivers and leaves the company exposed to risk from data oversharing and misuse.

If this sounds too familiar or you're worried about rushing to adopt Teams to support a remote workforce, relax. We have you covered. It is possible to reap the vast benefits of Teams collaboration — even in a hurry — without the governance and security headaches. We've recapped five tips from our recent webinar on how you can provision Teams with governance and information security built-in to improve adoption and ensure secure collaboration.

It's important to **understand** why **governance and security are so important** when it comes **to Microsoft Teams.** Collaboration tools like Teams have made it **easy** for **sensitive information** to be **accidently overshared** or fall into **malicious hands.**

Governance and data security importance

Before we share our tips, it's important to understand why governance and security are so important when it comes to Microsoft Teams. Collaboration tools like Teams have made it easy for sensitive information to be accidently overshared or fall into malicious hands for a few reasons:

1. The way we work has changed - quickly

Previous stats show that employees are more mobile than ever — from coffee shops to airports and hotels to homes, where 70 percent of the workforce works remotely one day a week. While no data exists on how many are working from home in light of the coronavirus pandemic, the 37 percent one-week gain in Teams users, as well as a sharp increase in Slack adoption, is a good indicator that more and more enterprise employees are now working from home.

2. How we access and share data has changed

Add to that the fact that we now work across functions, multiple devices, collaboration platforms and business boundaries with diverse teams made up of employees, contractors and suppliers. Information no longer resides within the virtual castle walls.

3. Unstructured data is vulnerable

Unstructured data — i.e. email messages, word processing documents, spreadsheets, videos, photos, audio files, presentations, webpages and other kinds of business documents — are no longer centrally located. Instead, multiple on-premises and Cloud channels are used to share this information, including email servers, file shares, SharePoint, Office 365, OneDrive, Microsoft Teams and Yammer chats, and BOTs. This makes it harder than ever to protect sensitive information like trade secrets, acquisition plans, financial data, supplier and customer information, and more from being shared too broadly, with the wrong person or team — inside or outside your company.

4. Traditional defenses and protection do not work

Perimeter defenses, legacy DLP and complicated permissions do not stop access and sharing of data by trusted insiders. They are primarily designed to keep insiders out, not protect data from misuse, theft or accidental sharing by your internal users that are meant to have access to it. As with anything, you need to use the right tool for the job — and these just don't cut it.

But I trust my users

We've all been focused on protecting our systems from hackers and bad actors on the outside for so long that it's sometimes hard to understand why tools like Teams make turning the focus inward equally important. Here are some sobering facts from a recent Nucleus Cyber and Cybersecurity Insiders survey on the current state of insider threats:

- *70 percent of organizations confirm insider attacks are becoming more frequent*
- *70 percent of companies are more worried about inadvertent insider breaches and negligent data breaches (66 percent), than they are about malicious intent by insiders (62 percent).*
- *39 percent identified cloud storage and file sharing apps as the most vulnerable to insider attacks*
- *85 percent of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack*

While many think insider threats are limited to malicious employees looking to steal from (or sabotage) the company, the simple truth is negligent employees or contractors can unintentionally pose an equally high risk of security breaches and data leaks by accident.

With that in mind, here are our tips for the five things you can do to roll out or retrofit Teams with governance and information security to fuel adoption and ensure secure collaboration.

1. FAMILIAR – Help your users

First, to set up Teams for success and ensure a smooth roll out, use provisioning or templates that are provided out of the box. Remember that with Teams, business owners, not just IT, can create new teams/channels. Template use ensures that teams are created with the proper governance and sharing rules in place, regardless of who's spinning up a Team. When it comes to the

David Salter *supports organizations in creating an agile, digital workplace by leveraging Microsoft 365, and all it has to offer.* david.salter@livetiles.nyc *@davidsalter365*

users, familiarity with Office products is great for getting started, but users still need guidance, tips and tricks, and other training over time to get the hang of it. Look to enlist existing early adopters for peer support efforts so that together your users can fuel adoption.

2. FAST – Speedy but setup for success

As companies look to quickly roll out teams, remember two impart points for success. First, make sure you start with security and compliance from day one. To help with this, create Teams based on fixed templates that have classification and metadata on Teams. Second, the side effect of anyone being able to create a Team is sprawl — including duplicate Teams and abandoned Teams. To avoid this, you should look to use automation for approvals, expiration reviews and orphan cleanup for expired Teams, to keep your implementation tidy.

3. INTEGRATED – Expand beyond files and chat

Teams is great for file sharing and messaging, but it can support so much more. You can add options for employee onboarding, learning management and HR/payroll directly into your Teams, for example. The best part is that you can keep users focused on their work, not the tech, by leveraging the Teams App catalog for system integrations, across major enterprise software apps.

4. CONTROLLED – IT must have visibility

Metrics are the key to a successful implementation. Having Teams data and analytics dashboards for IT and users is important to check on the health of your Teams. Auditing and reporting on adoption, growth in Teams numbers and content is important for maintenance, measuring engagement and making improvements. Be sure to create lifecycle guidance for users and automate notifications and lifecycle tasks as much as possible.

5. SECURE – You cannot sacrifice security and compliance

We'll say it again: the biggest threat to your information security and compliance program is accidental or negligent sharing of files and chat. It could be as innocent as sharing the wrong file in the wrong Team, and suddenly your merger plans are not so secret anymore. If you're in a regulated industry like financial services or healthcare, you need to ensure any required ethical walls and information barriers are in place to protect financial and patient information — and keep you out of trouble with the regulators. And in any industry, external sharing is almost always a necessity so make sure you have controls in place to limit what third parties can do with data they have access to. ■

Microsoft Teams Support Services.

We're here to help you get Microsoft Teams up and running for your work-from-home employees in hours, not days, using our unique governance model with support from our global team of Teams experts.

https://www.livetiles.nyc/teams-support-program

Microsoft Teams | LiveTiles