
EBOOK

# 8 TIPS TO PREVENT OVERSHARING AND INSIDER THREATS IN MICROSOFT TEAMS

archTIS

# EXECUTIVE SUMMARY

Microsoft Teams is rapidly becoming a key collaboration tool for many organizations and that trend will continue through 2020. However, many are expressing concerns that the rapid roll out is potentially leaving them exposed to data breaches and insider threats due to accidental sharing of the wrong files or information.

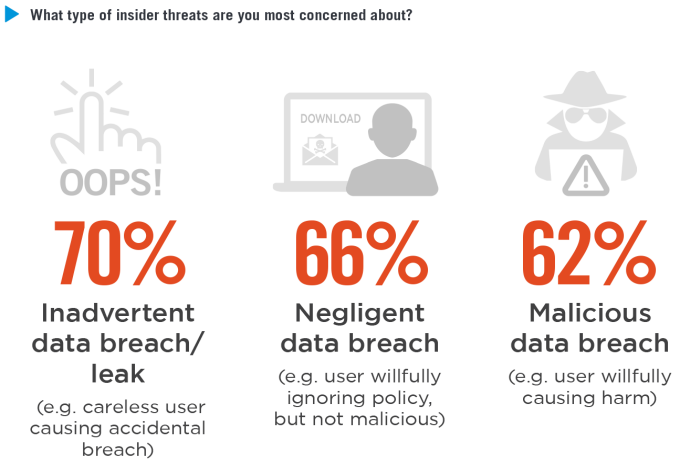
As a result, some deployments are being paused while organizations wrestle with how to address this issue. Customers in regulated industries are particularly caught in this quandary of satisfying user demands for the great collaboration benefits that Microsoft Teams brings and their legal responsibilities for appropriately handling sensitive information.

*What are the options for mitigating the risk to reap the rich collaboration features of Teams?*

Here's 8 tips to help prevent oversharing and the potential for insider threats in Teams so you can take advantage of productivity gains and increase user adoption - while ensuring collaboration is secure.

## INSIDER THREATS TAKE CENTER STAGE

**A recent report by Cybersecurity Insiders revealed most organizations are more concerned about internal threats than external attacks.***




## 1. DON'T DO THIS

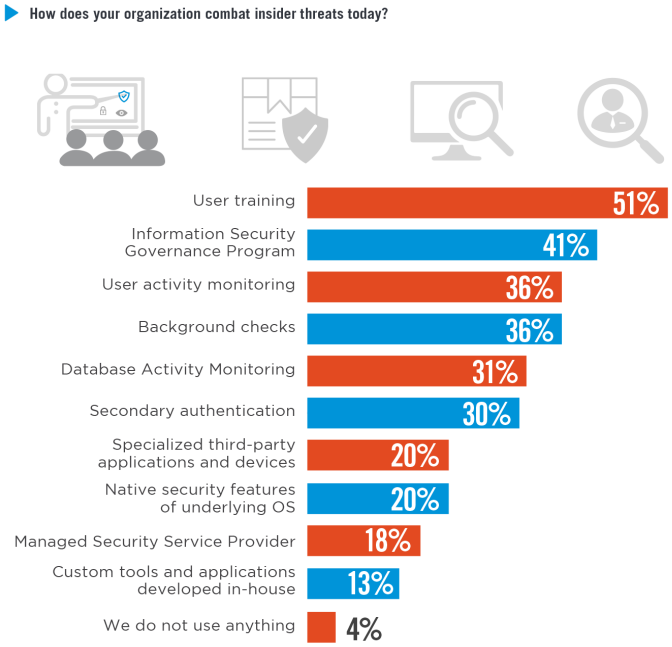
Before we get into some of the things that can be done to mitigate the risk, first let's look at an approach that is destined to fail: cutting off collaboration tools or making it too difficult for users to create and adopt Teams.

While this approach may solve the problem in the very short term, long term it is bound to cause frustration among end users and increase the risk of shadow IT as users look to work around overly restrictive IT control.

A common example is removing the ability to add external members to Teams. This approach is akin to asking users to circumvent Teams and IT. If there is a need for users to collaborate externally it is much better to find a solution within your corporate sanctioned tools rather than force users to seek their own solution.

There are many positives to embracing Teams for collaboration, instead we must look to how to mitigate the risks of accidental oversharing more effectively than opting for blocking its use.

**A recent survey by Cybersecurity Insiders highlighted how much organizations rely or plan to rely on user education to mitigate against 'insider threats'***




## 2. FOCUS ON THE USERS

A recent survey by Cybersecurity Insiders highlighted how much organizations rely or plan to rely on user education to mitigate against 'insider threats' – the industry term that includes the accidental oversharing scenario that we are discussing here.

It makes sense that user education should play a part in mitigation. After all, the security of business information assets is the responsibility of everyone in the organization. It would be unfair to place that responsibility on users without providing appropriate levels of education. However, as you can imagine, there are some potential flaws with this approach.

One issue is that regardless of how much training takes place, accidents will still happen. It's all too easy to put a file in the wrong location as users jump between their ever-increasing list of Teams that they have membership to. In this scenario it does not matter how much training has focused on the correct places to share information.

### The Top 4 Ways Data is Breached

1. An outside party breaks through the perimeter defences and steals the information
2. A bad actor discovers how to impersonate a trusted user and accesses information using the compromised credentials
3. A trusted insider maliciously takes information out of the company for their own personal use or gain
4. A trusted insider is negligent with their data handling despite what any user training or written policies state and accidentally shares or loses sensitive information

## 3. CHANGE UP TEACHING METHODS

It is not just about the amount of user education that takes place, but rather the type of training used to mitigate against accidental sharing. Remember that security is the responsibility of everyone within the organization and the burden of preventing accidents should not be isolated to the individual who uploads a file to the wrong location. Perhaps training for information handling in tools like Microsoft Teams could take a leaf from the anti-phishing book?

A common strategy for checking that users are aware of phishing techniques is for IT to send phishing emails to their employees as a test. For example, Microsoft uses a real message from their IT department and a “fake” phishing email. Users who are hooked are taken to a page that shows them the signs that they missed in the phishing email. As a result of adopting this strategy to supplement training Microsoft has seen a significant reduction in the number their users falling foul to real phishing attacks.

An adjusted approach could be used to test the awareness of users when it comes to sensitive information being shared within the wrong Team. Documents containing fake social security numbers, healthcare or financial information could deliberately be placed within a Team to see who accesses the file and if they take the appropriate steps e.g. alert the person who uploaded the file.

The success of anti-phishing tests in the real-world show that there is some merit in trying similar tactics to ensure that any training on information sharing practices has taken hold.

### How To Setup Microsoft Teams for Success

Leverage a provisioning process or tools for setting up Teams to:

1. Guide users to utilize Teams correctly based on how a Team is labeled or categorized
2. Remove the reliance on Team owners to ensure that sharing settings or tabs are correctly added or configured for the Team
3. Provide many of the properties that additional technologies can leverage to prevent accidental sharing

## 4. SETUP MICROSOFT TEAMS FOR SUCCESS

There are parallels between the rapid adoption of Microsoft Teams that we are experiencing now and the viral adoption of SharePoint during its early iterations. It's important that we learn from the early SharePoint years and not repeat those mistakes with Teams. The stakes for getting things wrong are far higher today. The ease and speed at which information can be shared and the severity of the penalties for incorrectly handling information demand a better rollout this time.

Organizations need to approach a Microsoft Teams rollout with the same thought process that ultimately became a SharePoint best practice – namely a more governed and controlled creation of Teams that has right the balance between user and IT needs.

A key to this is ensuring that Teams are setup for success from the moment that they are created. Leveraging a provisioning process or tools can help ensure it gets off to the right start. Although it requires a little work, there are capabilities provided by Microsoft to create templates that help to ensure that individual Teams are created with the appropriate structure and attributes e.g. can guest users be added or only allow internal users.

Although it may seem that the proper provisioning of a Team does little to prevent the original scenario, namely accidental sharing, it does create an appropriate foundation to support this effort in a few ways:

1. User training can be aligned to the approved use cases and associated templates so that users are guided to use Teams correctly based on how a Team is labeled or categorized.
2. It removes the reliance on Team owners to ensure that sharing settings or tabs are correctly added or configured for the Team. The news is full of data breaches that have been the result of an incorrectly configured cloud repository. Although Microsoft Teams by default has a more closed membership, and therefore access to the information within it, a risk still remains if the wrong users or group of users is added to the Team.
3. Creation of Teams through a provisioning process or tools provides many of the properties that additional technologies can leverage to prevent accidental sharing.

### Beware Private Channels

Private Channels do nothing to mitigate against the wrong data being placed in the wrong location. One could even argue they increase the risk of accidental oversharing.

## 5. TAKE CARE WHEN USING PRIVATE CHANNELS

There is one scenario where everything within the Team is not open to the entirety of the Team membership. Private Channels in Teams were introduced by Microsoft in response to the overwhelming demand from customers to be able to only have a subset of Team users be able to access certain information. Prior to the release of this feature the only option was to create a completely separate Team which forces users to jump between multiple Teams to satisfy a specific use case. Now users can create a channel within a Team that has a subset of members from the overall Team membership.

While this sounds like a step in the right direction by allowing users to make a conscious decision to share confidential information with a more easily controlled subset of users, in reality it doesn't solve the problem in its entirety. All we have done is create another information silo that once again relies on permissions - which we have shown is a single point of failure when it comes to accidentally placing files in the wrong location or granting access to the wrong users.

Private Channels do nothing to mitigate against the wrong data being placed in the wrong location or accidentally granting access to the wrong person. One could even argue they increase the risk of accidental oversharing. Users not only have to make sure they are placing files in the correct Team, but also have to make sure they are in the correct channel within the Team.

### Don’t Use Outdated Methodologies!

We need to accept that the nature of sensitive information and how we collaborate within organizations today requires us to tailor information security to our specific needs.

## 6. EMBRACE LESSONS LEARNED FROM OTHER SECURITY BEST PRACTICES

IT has embraced the fact that allowing access to networks or applications cannot solely rely on a single user name and password. Many organizations now leverage multi-factor authentication and CASBs to provide more secure and granular control over user access.

The same lessons must also be learned for securing access to valuable company data. This is particularly important for Cloud collaboration tools like Microsoft Teams where their ability to empower users to easily create and share files and information is arguably equally both their most valuable and most problematic attribute.

It’s important that we don’t just rely on the approaches that have been used with previous collaboration tools. User training and assessment of the effectiveness of training must adapt and make use of approaches that have been successful elsewhere.

Equally, we need to accept that the nature of sensitive information and how we collaborate within organizations today requires us to tailor information security to our specific needs. Inevitably this means seeking out tools that can provide granular data-centric protection that is not possible out-of-the-box due to one size fits most nature of the collaboration tools themselves. This is not a slight in anyway on, in this case, Teams itself but rather an acknowledgment of the world in which we live.

Microsoft Teams is a fantastic collaboration tool. In many organizations it has almost completely replaced email for internal, and in many cases external, communications and collaboration. The risk of accidental oversharing within Microsoft Teams is as a result of the ease and simplicity of creating a place to share and collaborate on information.


### One Size Fits Most Security

Today we are faced with a one size fits most or fits mostly offerings from application providers. With the stakes higher than ever for data breaches, it's important for organizations to be able to tailor secure collaboration to their specific needs based on both regulatory and organizational requirements.

## 7. MIND THE GAPS

There is little doubt that Microsoft has upped its game in relation to the speed at which they are innovating and releasing new features on their Cloud platforms. However, when it comes to Teams, it is still relatively new and gaps exist in features needed to fully secure collaboration. It's also worth noting that Microsoft Teams itself may never have the features that are needed to solve this issue. Instead, it will be other products within the Microsoft 365 platform that are required. Products that not everyone may have or be able to afford within their subscription.

Additionally, Microsoft is creating a single offering for every organization in the world. As a result, as with other IT tools, we are faced with a one size fits most or fits mostly. Today, when the stakes are higher than ever for data breaches, it's important for many organizations to tailor the fit to their specific needs based on regulatory and organizational requirements.

Out-of-the-box there are limited options for providing granular information protection controls to adequately cover all the scenarios that Teams supports, therefore organizations are forced into compromising either security policy or usability hence the stalling of roll outs because neither is truly acceptable. However, there are partner solutions available to supplement Microsoft 365 that provide the coverage needed to prevent insider threats.

For this reason, it's important to look beyond Microsoft into their partner ecosystem. This is where you can find solutions for provisioning Teams to save the trouble of having to build your own using the Microsoft building blocks. It is also where you find data-centric solutions that solve the problem of accidentally placing files in the wrong location or incorrectly setting user permissions on a data location.

### Bridge the Gap with Data-Centric Security

By default, the security boundary is the Team itself therefore once access is granted, by adding as a member or owner, the entirety of the Team and its information is open with one exception that will be addressed later. Since data-centric solutions leverage multiple attributes - of both the user and the data - more granular access to information is possible.

## DATA-CENTRIC SOLUTIONS HELP BRIDGE THE GAP

Most of the failures relating to accidental breaches are as a result of relying on single factors or attributes for controlling access to the information. Traditionally we have relied on permissions to grant access to information. A second layer was added that considered any classification applied to the data (DLP solutions). However, these approaches operate independently and only leverage two data points.

Today there are many other attributes that can be used to build proper conditional access to information assets. Much like the improvements that have been made for application access with Cloud Access Security Broker (CASB) solutions, the same is now true for access and usage rights at the data layer. This approach is known as data-centric security.

Data-centric solutions are particularly powerful when it comes to securing Microsoft Teams assets. Out-of-the-box the security boundary is the Team itself. Therefore, once access is granted, by adding as a member or owner, the entirety of the Team and its information is open with one exception that will be addressed later.

Since data-centric solutions leverage multiple attributes - of both the user and the data - more granular access to information is possible. This is how we can effectively mitigate against the accidental oversharing. Rules built upon multiple attributes that can prevent access to files.

A common use case is when a Team has Guest (or external) users. For example, suppose a Team is classified as ‘internal sharing only’ or a document is labeled as ‘internal only’. In this scenario data-centric rules can remove access to a file or all files marked ‘internal only’ as the ‘Guest’ user attribute would fail the conditional access requirements.

## START DYNAMICALLY SECURING YOUR TEAMS COLLABORATION

Discover how NC Protect secures Microsoft Teams collaboration and prevents oversharing risks with dynamic data-centric security based on real-time comparison of file content and user context.

For more information or a product demo visit www.archtis.com

## 8. EMPOWER USERS TO COLLABORATE FREELY WITHOUT RISKING SENSITIVE DATA

NC Protect offers a better way to secure your sensitive information by enhancing key Microsoft Information Protection (MIP) capabilities to provide fine-grained, data-centric security. The solution prevents accidental oversharing, misuse and theft of chat and file content in Microsoft Teams by enhancing out-of-the-box security with:

Conditional access and usage rights to prevent accidental sharing within Teams

Default application of organizational information protection rules upon a Team's creation

Unique, additional information protection capabilities such as user-specific watermarks and secure read-only access through a zero-footprint file viewer

If you're worried about or struggling to secure your Microsoft Teams collaboration contact us to learn more about how NC Protect offers greater protection and control over ALL your Teams and Office 365 content.

## ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS.com | info@archtis.com

Australia | United States | United Kingdom