

How to Secure Collaboration from Insider Threats

Rod Bray, Innovation and Experience Lead, LiveTiles

Steve Marsh, Vice President, Product, Nucleus Cyber

About us

LiveTiles is a publicly traded global cloud software company headquartered in New York with over 30 offices globally.

LiveTiles offers intelligent workplace software for the commercial, government and education markets, and is an award-winning Microsoft Partner.

LiveTiles has over 1,000 customers representing a diverse range of sectors and are spread throughout the United States, United Kingdom, Europe, the Middle East and Asia-Pacific.

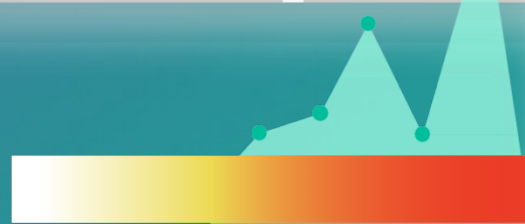
The dashboard features a top navigation bar with 'HOME | ABOUT | NEWS ROOM | TEAMS | PROJECT | SUPPORT' and a search bar. A sidebar on the left contains navigation options like 'INTELLIGENCE', 'BROWSE', 'PAGE LEVEL', 'HEATMAP', 'INSIGHTS', and 'SITEWIDE'. The main content area is divided into several sections:

- Welcome Back Jason:** Personalized greeting at the top.
- My Announcements:** A section titled 'Working together' with placeholder text and an image of two people.
- My Social:** A 'Yammer' feed with a search bar and a post by 'Richard Harding'.
- My Dashboard:** A 'Flight Expense' gauge chart showing a value of 522.
- Employee Spotlight:** A featured image of a woman in a white lab coat.
- My Newsfeed:** A news item about 'Scientists at Imperial College London'.
- My Team:** A small profile picture of a person.
- My Documents:** A list of documents, including 'Example of Word1.docx'.
- Trending Documents:** A list of trending documents, including '1-29-18 Updated Paul Reichold SDR opp'.

At the bottom right, there are two data visualization widgets:

- Page Views:** A line chart showing a trend over the last 7 days, with a total of 24.16K Page Views and a +20% increase.
- Active Users:** A line chart showing a trend over the last 7 days, with 1.2K AVG Daily Active Users and a +7% increase.

The HR Bot interface includes a chat window with a message: 'Hey! I am Awesome-O your AI assistant. I don't have ZED's dance moves, but please tell me how I can help today.' Below the chat are buttons for 'Reimbursement Request' and 'Leave of Absence Request'. A 'Request a Leave of Absence' form is also visible, with fields for 'First and Last Name', 'Email', 'Phone', and 'Number of Days Off'. A 'SEND' button is at the bottom right.



Insider Threats are on the Rise

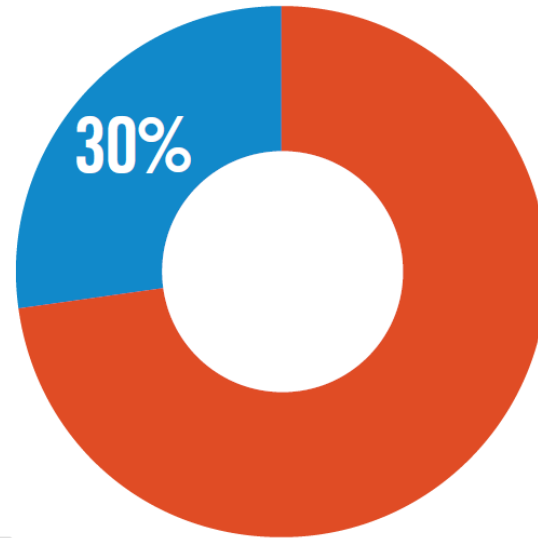
Key Findings

- 70% of organizations confirm insider attacks are becoming more frequent
- 68% feel extremely to moderately vulnerable to insider attacks
- 39% identified cloud storage and file sharing apps as the most vulnerable to insider attacks
- 85% of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack
- 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud



2019 Insider Threat Report

▶ Do you think insider attacks have generally become more frequent over the last 12 months?



70%

Think insider attacks have become more frequent in the past 12 months.

■ Yes ■ No

2019 Insider Threat Report

What type of insider threats are you most concerned about?



70%

Inadvertent data breach/leak

(e.g. careless user causing accidental breach)



66%

Negligent data breach

(e.g. user willfully ignoring policy, but not malicious)



62%

Malicious data breach

(e.g. user willfully causing harm)

Accidental Insider Threats

epoay

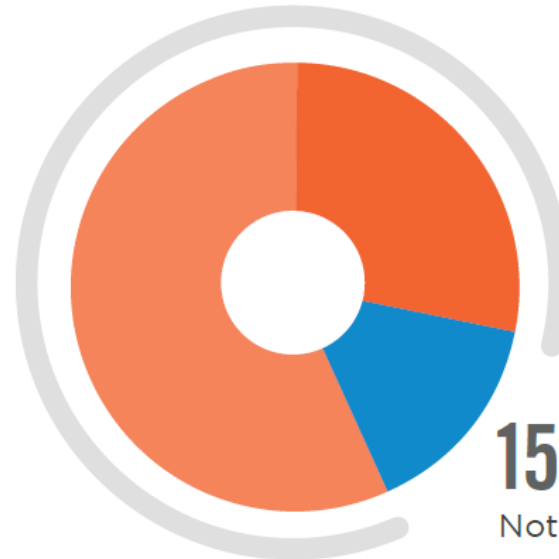


2019 Insider Threat Report

▶ Within your organization, how difficult is it to determine the actual damage of an occurred insider attack?

85% Find it moderately difficult to very difficult to determine the actual damage of an insider attack.

57%
Moderately
difficult



28%
Very difficult

15%
Not difficult

4 WAYS TO PREVENT INSIDER BREACHES



4 Ways To Prevent Insider Breaches



1. Find & Audit Your Data

Define what sensitive data is for your organization.

Identify where all your data currently exists – both at rest and in-motion.

Track all access to sensitive data as well as what actions that have been taken with it to provide a full audit trail.

4 Ways To Prevent Insider Breaches



2. Classify & Secure Data

Classify documents automatically based on the presence of sensitive.

Set business rules with your classifications to restrict actions that can be taken with classified documents such as print, email or save as to prevent data leakage.

Ensure that documents accessed on the mobile devices have the same security restrictions

4 Ways To Prevent Insider Breaches



3. Address Changing Risk Profiles

Users and data are not static – monitor changing attributes

Look at data on a continuous basis to monitor changing use cases.

Assess the risk profile associated with the data and its use cases, then consider the security that should be applied in each scenario.

4 Ways To Prevent Insider Breaches



4. Balance Collaboration with Security

Keep the right balance between user and organizational needs.

Too lax and your data can be shared far too freely.

Too stringent and your users find an alternative way to share and collaborate.

Use Case - Microsoft Teams

Microsoft Teams has incredible growth

- 20 million daily users and rising

All users can create a Team

- Great for users driving viral adoption

Limited out of the box Governance tools

- Not so great for Administrators

Empower Users to Work Efficiently and Securely in Microsoft Teams

Automatically
gain control of
governance,
security &
compliance

- All Teams automatically adhere to company governance, compliance, data-centric privacy and security policies upon creation
- Create Teams with the appropriate settings and metadata to ensure findability and systematic governance

Provide granular
data-centric
protection for all
your
collaboration

- Set-up Information Barriers between Team members to meet regulatory compliance
- Apply granular security to ensure sensitive/confidential files and chats are shared only with authorized internal and third-party individuals and groups
- Empower Team owners to apply additional granular protection over files and chat content directly from within the Teams UI reducing the need for IT resources

Prevent Teams
sprawl and keep
your O365
environment tidy

- Governance dashboard provides a full overview of all teams from a single place
- Users get a personalized dashboard with all the tools and information they need to get work done
- Automate review processes based on creation date or lack of activity within a Team to reduce clutter and wasted resources

Governance and Lifecycle control for Microsoft Teams

Create Teams based on fixed templates to ensure governance and security right from the start

Systematically collect metadata ensuring all teams are optimized for findability and governance

Automated tasks ensure timely review of members and content and that inactive teams are archived

Governance Dashboard shows all Teams and their metadata, inactive teams and those needing review

The screenshot displays the Microsoft Teams Governance Dashboard. The main view is the 'Workspaces dashboard' for the 'Wizdom' team. It features a 'Workspaces by Activity' pie chart and a table of workspaces.

Workspaces by Activity Data:

Activity	Count	Percentage
Low	7	36.84%
High	6	31.58%
Medium	3	15.79%
None	3	15.79%

Active Workspaces Table:

Title	State
AI	Archive
Astanga yoga	Active
Copenhagen running club	Archive
CRM restructuring	Active
Department IT	Archive
Homes - now and in the future	Active

Inactive Workspaces: No workspaces found.

Workspaces up for review Table:

Title	Sitetype	Owner	Review date
Astanga yoga	Collaboration		2019-03-05
Machine learning	Collaboration	Peter Parker	2019-09-29

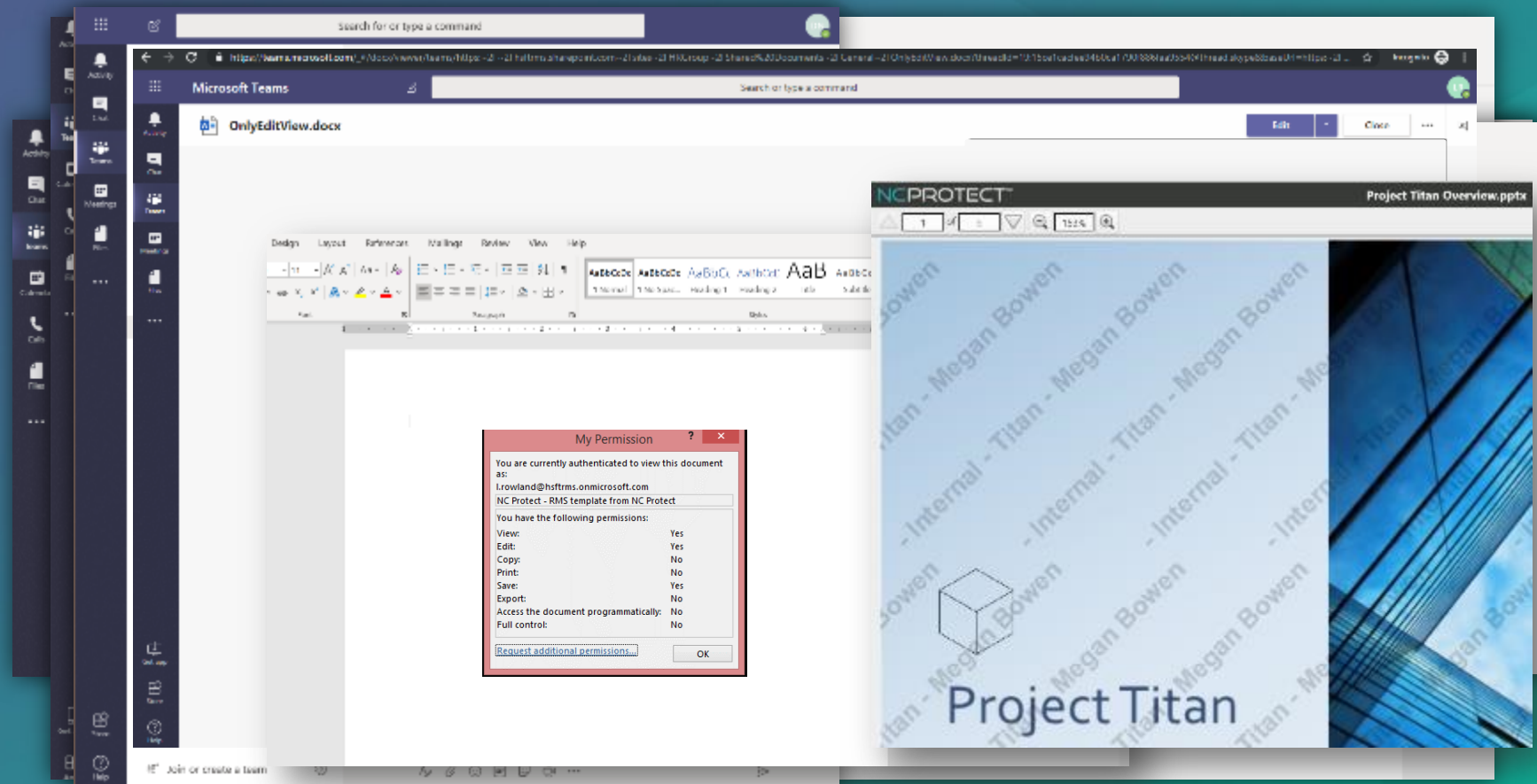
Dynamic Information Protection for Microsoft Teams

Automatically apply Information Protection rules when a Team is created

Empower Teams owners to create and apply their own Information Protection rules

Block chat or files based on content and user attributes to enable granular protection within Teams

Apply encryption and other usage rights dynamically to prevent accidental or malicious insider threats



Questions?

Steve Marsh

steve.marsh@nucleuscyber.com

www.nucleuscyber.com



Rod Bray

Rod.Bray@livetiles.nyc

www.Livetiles.nyc

