



7 Tips for Securing Marketing Cloud Engagement

in a Hybrid Work Environment



Learn. Network. Grow.

MParDreamin' 2022

7 Tip for Securing Marketing Cloud Engagement

Mike Morris

Sr. CRM & Marketing Automation Strategist, Sercante



Special Thanks To Our Sponsors



Title

SERCANTE



Platinum

D=SELECT

stensul

tray.io

Gold

FormAssembly

LeanData

STACK MOXIE

THE SPOT
FOR PARDOT by SERCANTE

Silver

MarketingOps

Goldcast

THE SPOT
FOR PARDOT JOBS

GREENKEY

FIONTA



The Rise of Hybrid Work Environment

Survey Says

A survey of over 9,000 workers conducted by Slack in October 2020 found...

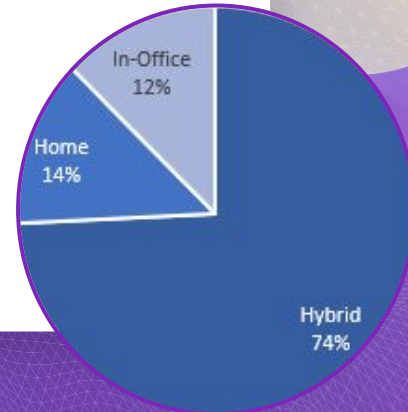
- 72% of workers prefer a hybrid model*
- 13% wanted to work at home full time
- 12% preferred working in the office full-time

*Home plus one or more other locations.

Source:

Moving beyond remote: Workplace transformation in the wake of Covid-19

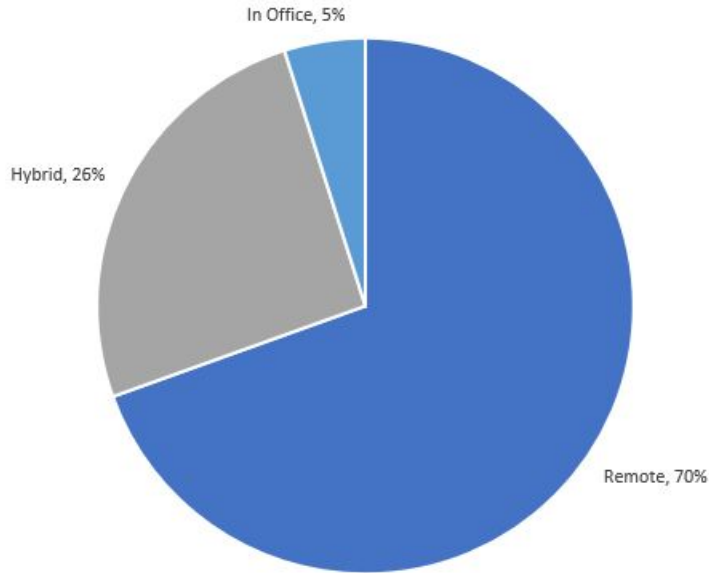
<https://slack.com/blog/collaboration/workplace-transformation-in-the-wake-of-covid-19>



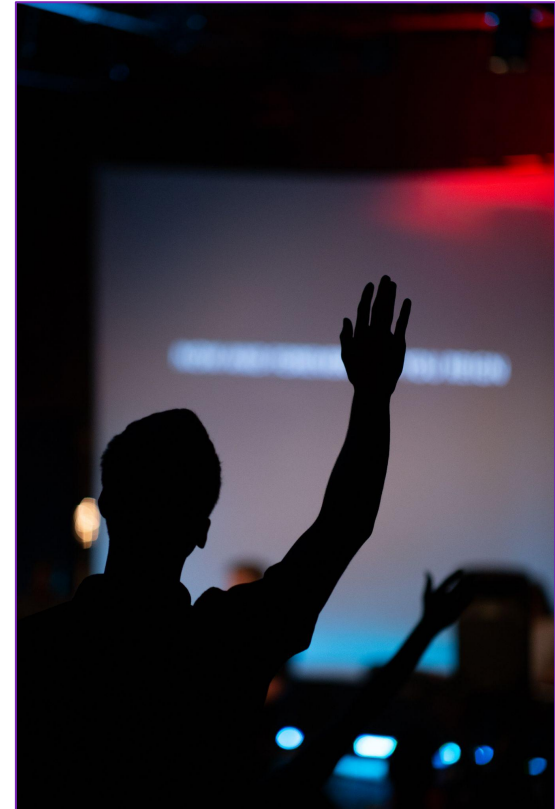
Florida Dreamin' Poll



What's your preferred working environment?



*Based on 82 responses



Benefits of a Hybrid Work Environment



- Workers experience more flexibility and better work-life balance
- Organizations gain the benefit of recruiting from a more geographically dispersed workforce
- Many studies also cite higher productivity and lower attrition rates as benefits for employers

While there are many benefits of a hybrid work environment, IT security is not one of them.

Security Challenges We'll Address Today



- Login policies and password strength
- Data security and data handling
- Unsecured devices



Login Policies and Password Strength

Tip #1 - Follow Login and Password Best Recommendations



Field	Recommended Setting
Session Timeout	20 Minutes
Login Expires After Inactivity	90 days or less
Invalid Logins Before Lockout	3
Count Invalid Logins Across Sessions	Yes
Minimum Username Length	8 characters
Minimum Password Length	8 characters or more
Enforce Password History	8 passwords remembered
User Passwords Expire In	90 Days
Send Password Change Confirmation Email	Enable
Enable Audit Logging Data Collection	Enable

Tip #2 - Limit Logins by IP Address



- Optional feature that can be enabled under [Setup > Security Setting > Username and Logins](#).
- When using this feature, the IP Allowlist must also be defined under [Setup > Security > Login IP Allowlist](#).
- Options to log non-allowed IP addresses and permit access or log non-allowed IP addresses and block access.

The screenshot shows the 'Setup Security Settings' page for 'Username and Logins'. The 'Restrict Logins by IP Address (IP Allowlisting)' checkbox is checked. A dropdown menu is open, showing options: 'IP Allowlisting Disabled', 'IP Allowlisting Disabled', 'Log Allowlist Violations' (highlighted), and 'Log Violations & Deny Access'. Other settings include 'Login Expires After Inactivity' (90 Days), 'Invalid Logins Before Lockout' (3), and 'Minimum Username Length' (6 characters).

The screenshot shows the 'Setup Login IP Allowlist' page. It features a 'View Access Log' button highlighted with a purple box. Below the button is an information icon and the text: 'The IP Allowlist automatically includes all Salesforce IP addresses.' At the bottom, a table header is visible with columns: 'Start IP Address', 'End IP Address', 'Description', and 'Login Source'.



Data Security and Data Handling

Tip #3 - Limit Data in Marketing Cloud



Salesforce Marketing Cloud is not a data warehouse. So don't treat it like one.

Before importing data or creating a data extensions, ask yourself one simple question...





***How will this data be used for
segmentation?***

Personally Identifiable Information



The Department of Homeland Security defines PII as:

As any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Depending on the type of data in your system and the industries that you serve, additional security measures like data at rest encryption, field level encryption and tokenized sending might be necessary.

Tip #4 - Limit Access with Business Units



Business Unit can be used to...

- Control access to information by creating a hierarchical structure
- Control branding elements
 - Email display name
 - Email reply address
 - Physical mailing address
- Allow unsubscribe at the BU or enterprise level

*Business Units are available in Enterprise and Enterprise 2.0 accounts.



Sample Business Unit Structure



Setup Business Units

Business Units

Create Delete | Manage Roles View Users Define Subscriber Filter Import | Show :

<input type="checkbox"/>	Name	Description	Parent Name	Number of Users
<input type="checkbox"/>	AMER	Americas BU	Sercante (Partner Main*)	2
<input type="checkbox"/>	EMEA	EMEA BU	Sercante (Partner Main*)	1
<input type="checkbox"/>	Sercante (Partner Main*)			5

BUs can be set up be region, line of business, or however your organization is organized.



How many many users have admin rights?

Tip # 5 - Utilize Permissions & Roles



Permissions are micro-level security.

- Example: The ability to Create, Edit in Journey Builder.

Roles are macro-level security.




- They are a collection of permissions.

A screenshot of the 'Setup Roles' interface in Marketing Cloud. The page title is 'Roles > Marketing Cloud Administrator'. Below the title are buttons for 'Save', 'Delete', and 'Cancel'. There are links for 'expand all' and 'collapse all'. The main content is a table with two columns: 'Allow' and 'Deny'. The table lists various permissions, some of which are expanded to show sub-permissions. The 'Automation' section is expanded, showing 'Create, Edit', 'Activate/Stop/Pause/Resume/Send/Schedule (journey state)', and 'Delete'. The 'Sales And Service Cloud' section is also expanded, showing 'Reports', 'HubExchange', 'AdobeAnalytics', and 'Tags'. The 'Allow' column has blue checkmarks for 'Create, Edit', 'Activate/Stop/Pause/Resume/Send/Schedule (journey state)', and 'Delete'. The 'Deny' column has empty checkboxes for all listed permissions.

	Allow	Deny
<input type="checkbox"/> Audience Builder	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> SocialEngage	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Salesforce Marketing Cloud	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Marketo	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DeveloperApp	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MobileConnect	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Automation Studio	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Email	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Discover	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> CampaignAnalytics	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Administration	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Audience Builder Enabler	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Xpress	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Approvals (Email)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Distributed Sending	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MobilePush	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Journey Builder	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> General	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Automation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create, Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Activate/Stop/Pause/Resume/Send/Schedule (journey state)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Sales And Service Cloud	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Reports	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> HubExchange	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> AdobeAnalytics	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Tags	<input type="checkbox"/>	<input type="checkbox"/>

Permissions & Roles



Option	Description
	Permission Granted
	Permission Denied
	Permission not Explicitly Granted or Denied

When a permission is not explicitly granted or denied, Marketing Cloud defaults to a deny permission unless another role grants that permission.

Marketing Cloud Roles



Marketing Cloud Role	Description
Marketing Cloud Administrator	This role assigns Marketing Cloud roles to users and manages channels, apps, and tools.
Marketing Cloud Viewer	This role views cross-channel marketing activity results in Marketing Cloud.
Marketing Cloud Channel Manager	This role creates and executes cross-channel interactive marketing campaigns and administers specific channels like Email Studio.
Marketing Cloud Security Administrator	This role maintains security settings and manages user activity and alerts.
Marketing Cloud Content Editor/Publisher	This role creates and delivers messages through applicable channel apps.

Email Studio Roles



Email Studio Role	Description
Administrator	Access to all Email Studio functions including Setup, email creating, and creating data extensions.
Content Creator	Access to all content, shared folders, and tracking in Email Studio, but no access to data or administrative features.
Data Manager	Access to everything in Email Studio except email content
Analyst	Access to tracking features in Email Studio.

Multiple Role Assignment



Marketing Cloud Engagement [defaults to the most restrictive](#) value when multiple roles are assigned to a user.

Example:

If a user was assigned the Content Creator, Marketing Cloud Channel Manager, and the Marketing Cloud Viewer roles, they would not be able to send an email. This is due to the fact that the Marketing Cloud Viewer is the most restrictive of the three roles and does not permit email sending.

Tips for Assigning Roles



- Use the default roles included in your account if possible.
- When assigning roles to users, you should always start with the lowest level that permits the individual to do their job.
- Restrict the number of users assigned the Marketing Cloud and Administrator roles.
- If multiple roles are assigned to the same user, the most restrictive role will honored.
- The same user can have different roles in multiple business units.



Unsecured Devices

Who Should Have Access to Your Data?



While data in the hands of a user can be risky, the real concern is data sitting on a computer that is not properly secured.

Once the data leaves Marketing Cloud Engagement, [all bets are off.](#)





Does the user's job require data extracts?

Tip #6 - Limit Email Exports



- Export Email Allowlists define individual email addresses or domains that are authorized to receive email exports from your account.
- This feature must be activated by enabling Enforce Export Email Allowlist in Security settings.
- The list of allowed emails and domains must also be defined under [Setup > Security](#).

Setup
Export Email Allowlist

Export Email Allowlist

★ Create ✎ Edit 🗑 Delete

<input type="checkbox"/>	Address
<input type="checkbox"/>	mike.morris@sercante.com

Setup
Domain Allowlist

Domain Management

Automatically include all Salesforce domains [Learn More](#)

Add your custom domains and activate this feature to allow the domains.

Domain Name	Allow Subdomains
sercante.com	<input type="checkbox"/>

Tip #7 - Limit File Transfers



- Data can also be exported using file transfers.
- Access to the data can be controlled by limiting users and not sharing login credentials.
- Users can be granted Read Only or Full access.

FTP Site Information

URL
mcl2rq3jdt72pzk-cx6jf80xtf0m.ftp.marketingcloudops.com

FTP Users

1/10 accounts used [Add FTP User](#)

FTP Username	Status	E-mail Address	Port	Permissions	Password Expiration Date
514001685_2	Enabled	mike.morris@sercante.com	22	Full	12/29/2022
514001685	Locked	admin@sercante.com	22	Full	⚠️ 6/21/2022



Summary

Summary



- Hybrid work environments have many benefits for employees and organizations, but could compromise security.
- Marketing Cloud Engagement includes a robust set of tools that can be used to mitigate security risks - regardless of work location.
- Restricting account access, limiting data in the system, and controlling who can perform extracts are some of the best ways to protect your organization.

Special Thanks To Our Sponsors



Title

SERCANTE



Platinum

D=SELECT

stensul

tray.io

Gold

FormAssembly

LeanData

STACK MOXIE

THE SPOT
FOR PARDOT by SERCANTE

Silver

MarketingOps

Goldcast

THE SPOT
FOR PARDOT JOBS

GREENKEY

FIONTA



Thank you!

We appreciate your attendance at this session. If you have any questions please reach out to us via Goldcast or use the information below. We hope you enjoy the rest of the conference!

Mike Morris
mike.morris@sercante.com