ISSUE
01
FY 2020

JOURNAL OF INFORMATION TECHNOLOGY

# Tech Myth Busters

5 Minutes of IT Dose that securely empowers your business

This issue



## Work from Home

With the recent lockdown throughout the country, most organizations had to allow employees to work from home, conduct their meetings using video conferencing tools and adjust to the new norm.

Did you know that attacks on critical IT infrastructure has gone up by 30% just during the lockdown period?

Is your organization immune to such risks?

What precautions has your organization taken to recover should it become the target?

ZOOM-VIDEO CONFERENCING made a lot of fans because of its ease of use and free offerings but subsequently received a lot of bad press, arising out of security concerns on their platform. Should your organization abandon ZOOM and look for an alternate? Is it safe to use? We bust all the myths in this newsletter so you can take an educated decision.

## Zoom Video Conferencing Myths & Facts

| MYTHS | FACTS |
|---|---|
| ZOOM IS UNSECURE and THUS UNFIT FOR MY ORGANZIATION | ZOOM is secure but needs the meeting moderator to be informed of the settings that needs to be enabled for the meetings. It is fit for any organization except for certain government offices & industries serving them like defense, intelligence, where concerns of highly confidential & privilege information access is paramount. |
| ZOOM CAN SEE MY STORED/ RECORDED MEETING VIDEOS | If the stored/recorded videos are password protected ZOOM cannot see or access them.; If they are stored locally, it further improves security - BUT if the stored videos are left unprotected – there is no remedy. |
| ZOOM HAS HUGE PRIVACY CONCERNS | ZOOM has the following independent industry certifications to prove they are serious about privacy and security of their customers data.<br>• GDPR, CCPA, COPPA, FERPA and HIPAA Compliant (with BAA)<br>• SOC 2 (Type II)<br>• FedRAMP<br>• Privacy Shield Certified (EU/US, Swiss/US, Data Privacy Practices)<br>• TrustArc Certified Privacy |

ZOOM did have initial lapses (in Feb/March) when they focused more on ease of use rather than security, but since then they have improved significantly and offer one of the best in class solution that is highly secure and continues to be the most value for money alternate to others that are out there in the market. Like with any software, user awareness is equally important and on next page we provide simple yet specific recommendations for you to enable and make your zoom as secure as it can be.

Zoom offers free and paid version – the paid version enables the host to conduct meetings without limitations vs. the free version. We recommended to get at least one paid version ($15 per month payable monthly) as only the organizer/host needs the license while attendees don't need to purchase or pay for anything to participate in any video conferencing/meetings.


## Maze Ransomware

Ransomware attacks are on the rise as more home based personal (and thus vulnerable) computers, laptops, and iPads are now connecting and challenging secured corporate networks. Maze Ransomware has affected small and large organizations rapidly and taken organizations for a tail-spin.

THE ONLY SURE WAY TO RECOVER IS TO HAVE MOST RECENT / UPDATED OFFLINE BACK-UP OF YOUR CRITICAL DATA.

# Recommended Zoom Settings for Meeting Host/Moderator

### Pre-Meeting Settings

1. Enforce Waiting Room
2. Enable Unique Password to join for EACH meeting.
3. Only allowed authenticated users – recommended only for Board Meetings or meetings that share confidential data.

### During Meeting Settings

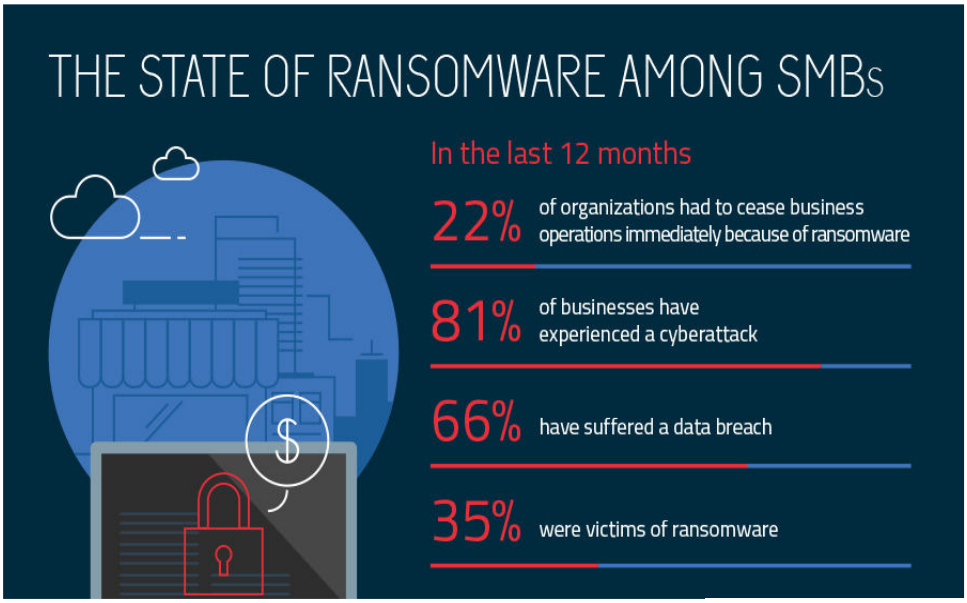
4. Lock Meeting – once all participants have joined, you can lock so no one else, even if they have the meeting ID/password won't be able to join.
5. Disable Private Chat
6. Turn-off File Sharing – If meeting content is to be distributed use company email or intranet instead of zoom file sharing for additional security.

### Post Meeting Actions

7. Recording Storage – if meeting recordings are stored on cloud or locally, password protect each recording.
8. Cloud Storage Access – Ensure cloud access to meeting data is NOT set to public. It should be set to internal-only allowing only authorized and authenticated users to access it.

## Recommendations to avoid and recover from Ransomware

1. Store all data in password protected / encrypted form
2. Ensure good malware protection is enabled/updated and working on critical servers.
3. If possible, place data servers behind a good internal firewall.
4. Ensure at least two copies of data is available – one preferably offline.




*Source Malwarebytes Industry Statistics*

**TECHNOLOGY CONSULTING DIVISION**

R. S. PATEL & CO.
CHARTERED ACCOUNTANTS

**Tech@RSPatelCA.com** **Ketul@RSPatelCA.com**

801 Popular House, Nr. Income Tax Circle, Ashram Road, Ahmedabad 380014 Tel: 079-26588909, 26585550