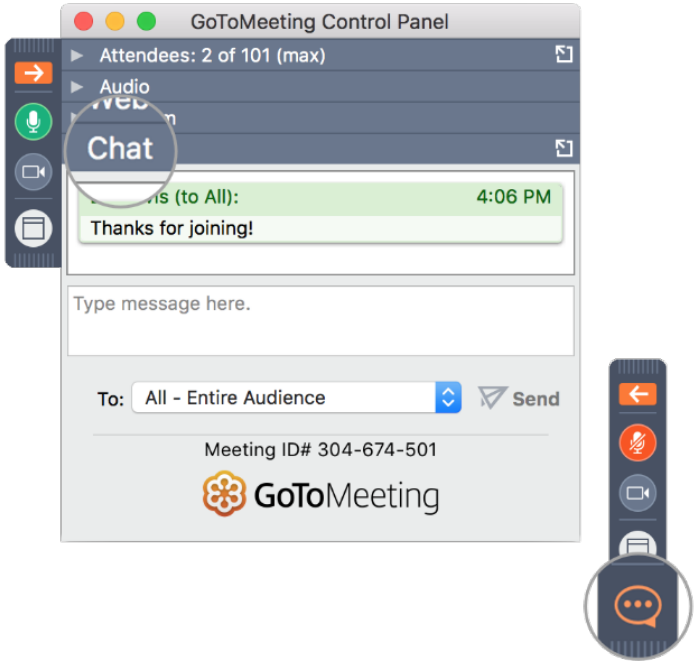
Addressing Technology Challenges Introduced by the COVID-19 Pandemic

Friday, April 10, 2020

Webinar Instructions

+Please submit questions through the Chat Box in the webinar control panel



Presenter

Nate Deskins

Partner/Director of Operations

Richard Taylor

Assurance Principal

General Overview

- The COVID-19 pandemic has changed the way people work and where they work.
- Technology is more essential than ever as companies quickly shift to an almost fully remote workforce.
- Many companies do not have the technological resources or business processes in place to deal with the quickly changing work environment. This can lead inefficiency and an increase in cybercrime.
- With so many options out there, it can be difficult to know what solutions to implement not just to stay functional, but to remain secure.
- We're here to help!

Preparedness

Most businesses are not prepared to be completely remote.

+ Identify the gaps
+ Update your “How-To’s” (Policies and Procedures)
+ Implement the *right* technologies
+ Establish regular training

Identify the Gaps

- What new challenges are presented when your team is never in the office?

- How can these challenge be addressed?
  - Policies/Procedures
  - Technology

Update your "How-To's"

- What changed when everyone went home?

- How do you.....
  - Manage team performance?
  - Complete essential job functions?
  - Pay your bills?
  - Receive payments from clients?
  - Answer the phone?
  - Check your voicemails?
  - Communicate with your internal team, clients and vendors?
  - Obtain technology support?
  - Keep your systems secure, patched, and up to date?

What are the right technologies?

All giving away free stuff

Establish Training Programs

- Training is low-cost/high reward, yet historically looked over
- Your team must re-learn how to complete job functions remotely
- Training should become a regular part of the work week

Remote Workforce Transition

Functionality

Has technology in your organization allowed you to function remotely with adequate security?

- Your technology should provide your team the ability to fully function from outside the office as if they were inside the office, while retaining the same level of security.
- Consider the risk of functionality vs security requirements.
- Governance and workflow policies, and procedures may need to adapt to ensure there is a solution in place for every job function that must be completed.

Communication

Are you able to communicate effectively with your internal team, vendors, and clients using your current solutions?

- Policy and ongoing status updates should be provided to your remote workforce to outline communication rules.
- Standardize communication solutions. That are approved by the organization.
- Cloud based phone and video conferencing solutions are not all created equal, and it's critical that the solution you invest in is robust enough to support the needs of your team safely as well as fit your budget

Functionality vs. Security

- Unprepared businesses have taken a knee-jerk reaction to COVID-19 by throwing together solutions to ensure that their team has access to work from home.
- Due diligence has not been performed, testing has been forgotten, and security has been an afterthought.
- Users are in an emotional situation and outside of their comfort zone

Security Awareness and Technology Support

First Line of Defense

- Employees are your *strongest* line of defense and your *weakest* link.
- The threat landscape is changing as our work environment is changing
- Now is not the time to forego security training!

IT Support Structure

- Whether your IT support is internal or through an outside vendor, everyone's support processes have been challenged during COVID-19.
- It's imperative that you coordinate and communicate with your team when support is available, if onsite support is an option, what are the limitations of support (i.e. would you support a home user's internet connection?), etc.

Monitoring Systems

- It is imperative that your IT team continues to have the ability to monitor all company owned equipment, access, and has a solid patch management system in place to keep your software up to date

- Don’t use non-monitored equipment (i.e. Personal).

Vendor Management

- Ensure policy's on vendor due diligence remain active. Many technology vendors have come forward in this time of need to offer free or long-term trials of popular products, designed to accommodate the new 'norm' of working from home.
- Re-assess vendor risk levels. Have vendors operational changes increased risk to your information? Do you need to review more often
- Review service level agreements. Have / Will these change?
- Understand specific communication / notification processes. Are you sure its your vendor communicating?

IT Support

- Do you truly understand the state of your network?
- Are you asking the right questions?
- How do you validate the information you receive.?
- Is a change management process still in effect?

Business Continuity Planning and Continuance (BCP)

Business Continuity Planning:

"Is a document that outlines how a business will continue operating during an unplanned disruption in service. It's more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, human resources and business partners – every aspect of the business that might be affected."

+ It's critical that your business has a plan in place to adapt to the quickly changing environment due to COVID-19.

Source: IBM

Is your BCP working?

- Did your company have a plan to address a pandemic outbreak?
- Document what is working and what isn't working.
- Prioritize essential business functions and processes.
- Expand your HR policies:
  - Up to date with federal regulations?
  - Staffing disruption
  - Payroll
  - Healthcare
  - Absenteeism

Is your BCP working?

- Ensure that legal and regulatory requirements are identified, documented and reported.
- Evaluate your dependencies on third party service providers.

What should we be now?

- Complete a comprehensive business impact analysis.
- Evaluate third party relationships.
- If you are in a regulated industry should you have activated your Incident Response Plan?
- Non-regulated industries should consider review of supply agreements, manufacturing agreements, distribution agreements, production agreements and general services agreements form both a send and receiving position.
- Whether creating or updating a BCP plan ensure it covers all aspects of you business.

Video Conferencing

Best Practices-As a Host

- Know your software!
- Test your hardware and internet connection before each meeting
- Create a professional environment
- Dress for your audience

Best Practices-As an Attendee

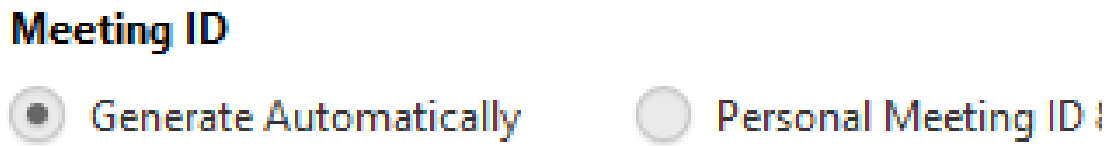
- Mute your microphone when you are not speaking, even if you are by yourself.
- Position your camera to be eye level and look at it straight on. Weird angles can be distracting and unflattering.
- Make sure your room is well lit.
- Wear appropriate clothing.
- Ensure everything in your room is work-appropriate.
- If you are in a group call, audio only, introduce yourself before speaking. If a large meeting, introduce yourself even with video as not all users will be visible on the screen.
- Pay attention! If on a video call, other attendees can see you performing other tasks. Keep focused, even If the speak isn't engaging.

What Happens on Your Call, Doesn't Stay on Your Call

- Many telecom services offer true 'end to end' encryption, but some do not
- **Don't say or show anything you wouldn't want to be repeated.** This includes Personally Identifiable Information (PII) as well as Protected Health Information (PHI)

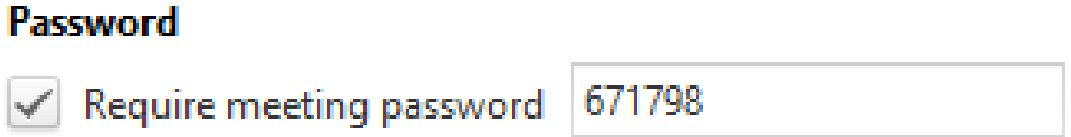
Meeting Security

- Create private meetings:
  - By generating a random Meeting ID for every meeting, you lower the risk of someone unexpectedly dropping into your meeting, especially if you are advertising the meeting publicly



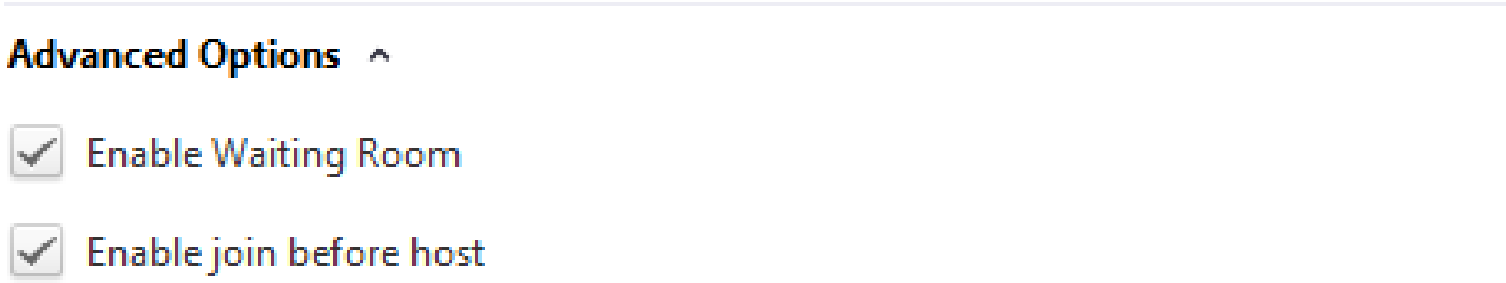
Meeting Security

- Use passwords to protect your meetings:
  - By keeping your meeting password protected, you add a layer of protection to keep people from ‘Bombing’ your meeting.



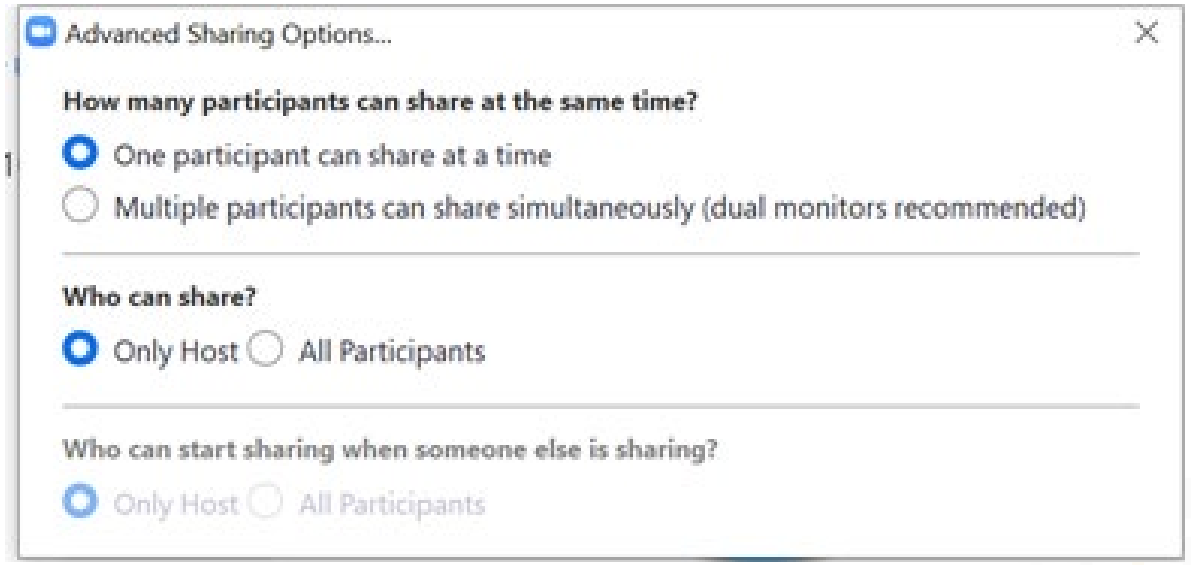
Meeting Security

- Use waiting rooms:
  - By enabling waiting rooms as the host, you have the ability to confirm the identity of every user before allowing them into the meeting.



Meeting Security

- Manage your participants:
  - As the host, you have the ability to manage your participants, which means controlling who can share their screen as well as who can and cannot speak.



Questions?

Please submit questions in Chat Box

Thank You

for your time!