ILLINOIS MANUFACTURERS' ASSOCIATION

Managing a Remote Workforce

Email questions for presenters to IMA@IMA-Net.org

BOLDLY MOVING MAKERS FORWARD

REMOTE WORKFORCE

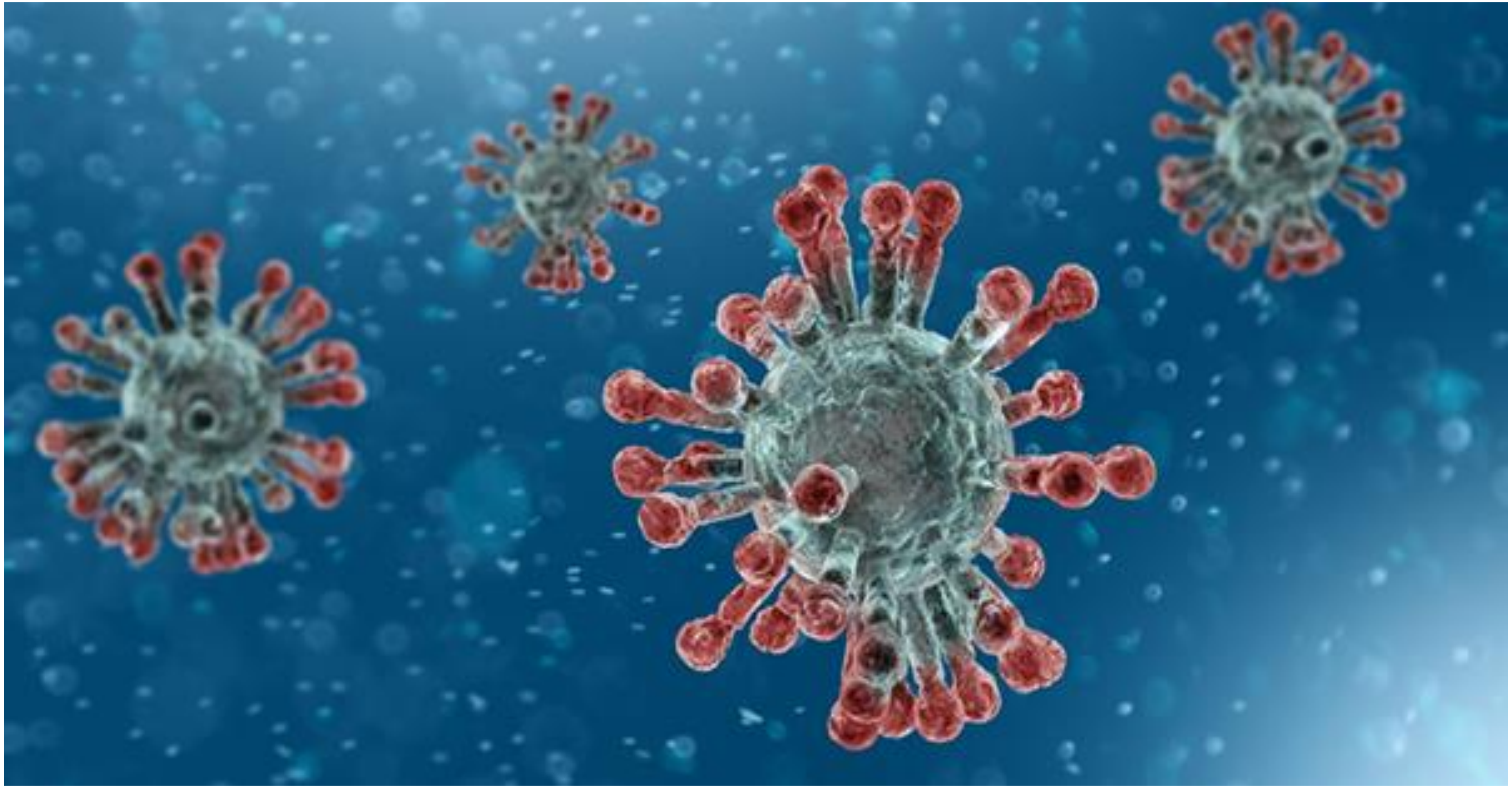
BEST PRACTICES FOR ENGAGING REMOTE WORKERS AND RE-EMERGING WORKERS INTO THE WORKFORCE

Presented by:

Jennifer Kramer, M.S., PHR, SHRM-CP

May 8, 2020

INTRODUCTION



AGENDA

- Managing Remote Workers
  - Pros/Cons
  - Legal Issues
  - Policies/Procedures
  - Keeping Employees Engaged
- Re-emerging Workers into the Workplace
  - When to re-open
  - Risk Assessment
  - Safety

PROS
?
CONS

LEGAL ISSUES

LEGAL ISSUES

POLICIES
PROCEDURES

POLICIES/PROCEDURES

KEEP EMPLOYEES ENGAGED

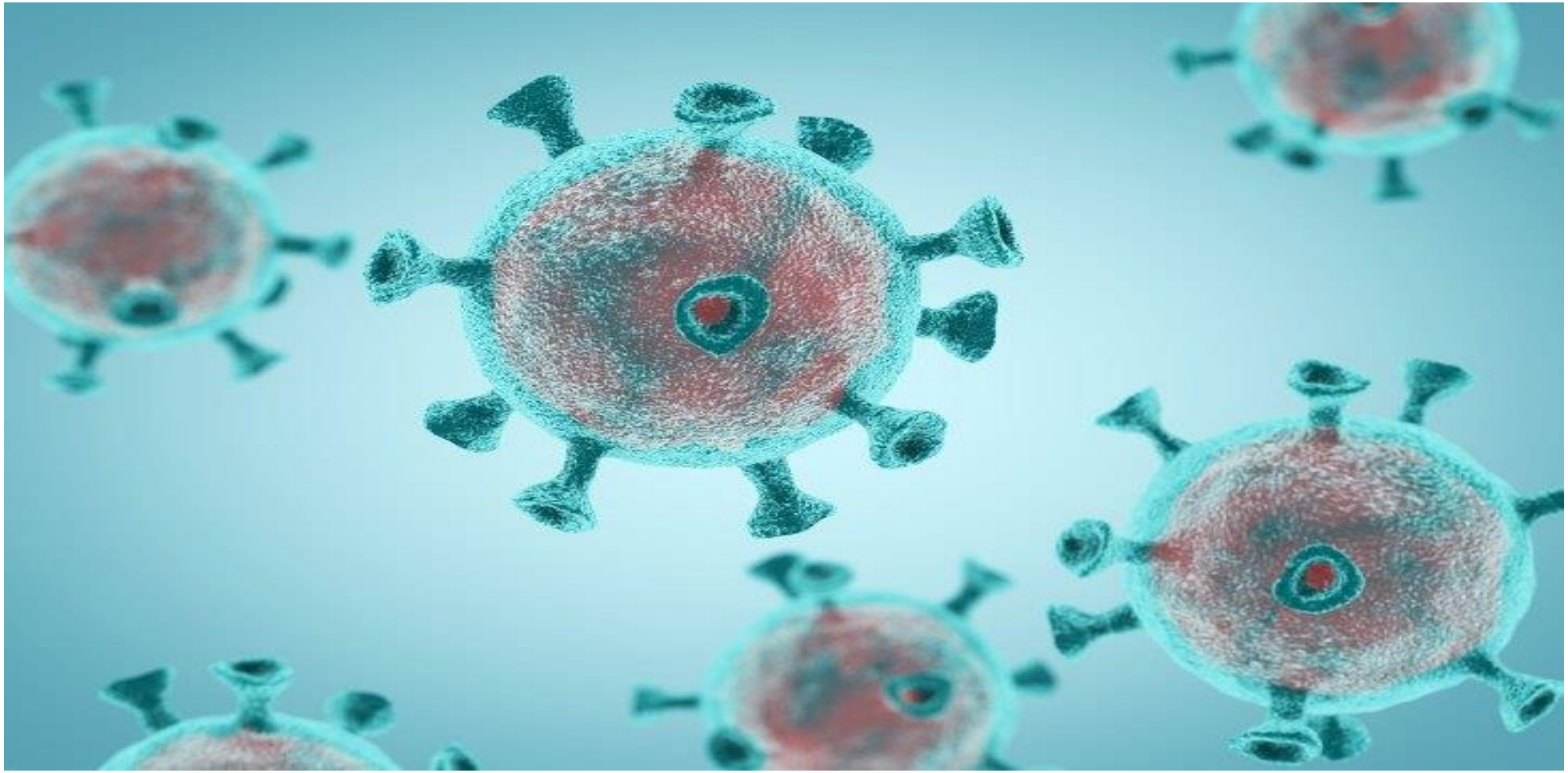
WELCOME EMPLOYEES BACK TO WORK

RETURN TO WORK PLANS

CONSIDERATIONS

CONSIDERATIONS (Cont.)

REFUSING TO RETURN



CONTACT INFORMATION

Jennifer Kramer, M.S., PHR, SHRM-CP

jkramer@presidiogrp.com

630.212.5265

THE POWER OF BEING UNDERSTOOD

RSM

CYBERSECURITY UPDATE – MAY 2020

Changes, threats, and risks with COVID-19

Speaker

Zach Raizen

Director

Zach is a cybersecurity professional with over 10 years of experience in a variety of areas including: technical security and penetration testing, security governance, privacy, emerging technology risk, and compliance assessments, such as PCI, NIST, HIPAA, and others.

Email: zach.raizen@rsmus.com

Agenda

- What is different?
- Different Risks
- New Threats
- Examples of Attacks
- What Should We Do?

What is different?

- Highly remote work means more use of teleconferencing/videoconferencing
  - Potentially including new technologies (Facebook Messenger rooms, Google Meet, Zoom, WhatsApp)
- Greater use of remote access technologies
  - VPN
  - RDP
- Use of home networks or other devices for network access
- Changes to business processes
  - How have paper based processes changed?

Different Risks

- Increased bandwidth use
- Videoconference disruptions (Zoombombing)
- New social engineering vectors
- Hardware availability/remote support
- Less defined network boundary
- Distancing and physical access controls
- Compliance obligations still in place (PCI, DoD DFARS, privacy, etc.)

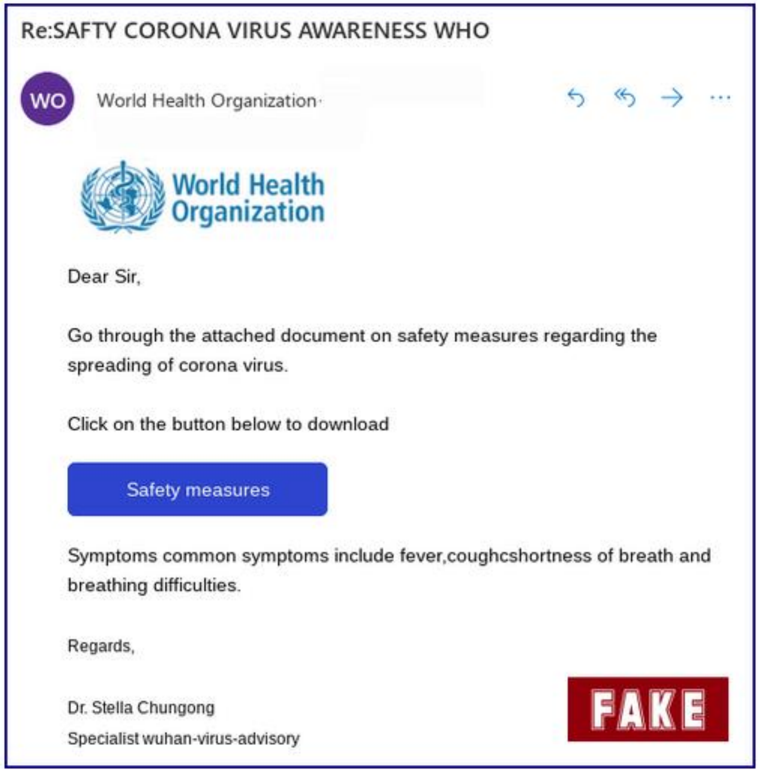
New Threats

- Attackers using the situation to their advantage:
  - Phishing emails for fake virus tracking sites, safety guidelines, Netflix payment expiration, etc.
  - Attacking processes that are in flux
  - Attacking processes that are now manual instead of automated
  - Targeting VPN endpoints
  - Attacking videoconferencing platforms

COVID-19 Cyber Attacks

Phishing

- No new technical attacks, just twists off of old favorites
- Pretending to be emergency authorities making announcements
  - CDC, WHO, Federal (
- Pretending to be com
  - HR announcements: E ,
  - C-Level: Emergency a donations, etc.
- Pretending to be law (
  - Curfews, lock-downs, e.g. riots)
  - Notification of death o



Re:SAFTY CORONA VIRUS AWARENESS WHO

World Health Organization·

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

COVID-19 Cyber Attacks

Process Attacks

- Attackers realize that many corporate communications and processes are under rapid alteration to accommodate remote work and lack of communications
- Attacking processes that are already being altered
  - E.g. “So and so is out of pocket because their connectivity is down, please approve this invoice in their stead.”
- Attacking processes that have been forced into manual mode because platforms, people, or processes are now unavailable
  - E.g. Banks overloaded with phone calls, slow to respond to requests, so attackers pressure employees to bypass controls to directly move payments

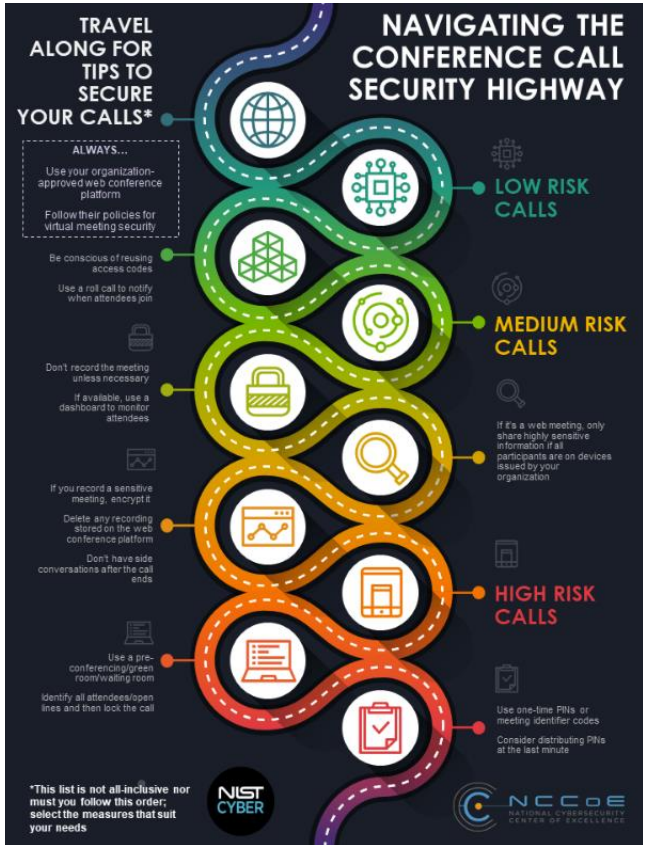
RSM

COVID-19 Cyber Attacks
Technical Attacks

- Many organizations were not structured for mass remote work
- Attackers realize this, and are rapidly escalating attacks looking for new/misconfigured/overloaded/etc. remote access solutions
- Similar wave of attacks for web based email, document sharing, and cloud instances
- Be very aware of your remote security infrastructure
- Attackers know that many employees are now working outside of the corporate security bubble, which leaves local AV as the last line of defense
- This is leading to a resurgence of “oldies but goodies” attacks

What should we do? (Videoconferencing and conference calls)

- Always set a meeting password
- Don't share links to meetings on public sites
- Use a pre-conference waiting room
- Consider the meeting material
- Use a roll call to identify attendees when joining
- Don't record meetings unless necessary
- Watch out for side conversations



TRAVEL ALONG FOR TIPS TO SECURE YOUR CALLS*

NAVIGATING THE CONFERENCE CALL SECURITY HIGHWAY

ALWAYS...

Use your organization-approved web conference platform

Follow their policies for virtual meeting security

LOW RISK CALLS

Be conscious of reusing access codes

Use a roll call to notify when attendees join

MEDIUM RISK CALLS

Don't record the meeting unless necessary

If available, use a dashboard to monitor attendees

If it's a web meeting, only share highly sensitive information if all participants are on devices issued by your organization

If you record a sensitive meeting, encrypt it

Delete any recording stored on the web conference platform

Don't have side conversations after the call ends

HIGH RISK CALLS

Use a pre-conferencing/green room/waiting room

Identify all attendees/open lines and then lock the call

Use one-time PINs or meeting identifier codes

Consider distributing PINs at the last minute

*This list is not all-inclusive nor must you follow this order; select the measures that suit your needs

https://www.nist.gov/image/conference-call-security-graphic

What should we do? (High Level)

- Now:
  - Review and update your risk assessment
  - Do not ignore normal security practices
  - Review the internal network, ensure layers of controls
  - Continue to educate users on new phishing threats and key controls

- Future:
  - Consider expanded remote workforce continuation
  - Create a low touch environment – minimizing contact for physical access
  - Update BCP/DR plans to include fully remote workforce

THANK YOU FOR YOUR TIME AND ATTENTION

RSM

RSM US LLP

1 S Wacker Drive, suite 800
Chicago, IL 60606
312-634-3400

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

IMA

ILLINOIS
MANUFACTURERS'
ASSOCIATION

IMA Recommended COVID-19 Online Resources at:

https://ima-net.org/covid-19/

BOLDLY MOVING MAKERS FORWARD