



# Securing The New Normal: Tackling Challenges of Remote Working and Learning

**Ang Leong Boon**

Head of IT Security

National University of Singapore

28 August 2020

# About Myself



- ▶ Head of IT Security at National University of Singapore
- ▶ Looking after security governance, risk management, security operations, user awareness, incident response
- ▶ >15 years of experience in cyber security
- ▶ Interest in speaking at conferences and giving guest lectures



**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



**ISACA**  
Singapore Chapter

# Agenda

- ▶ Emerging challenges from COVID-19
- ▶ Risks from home networks
- ▶ Attacks on corporate networks
- ▶ Remote access solutions compared
- ▶ Secure video conferencing
- ▶ Conducting e-Learning and e-Exams



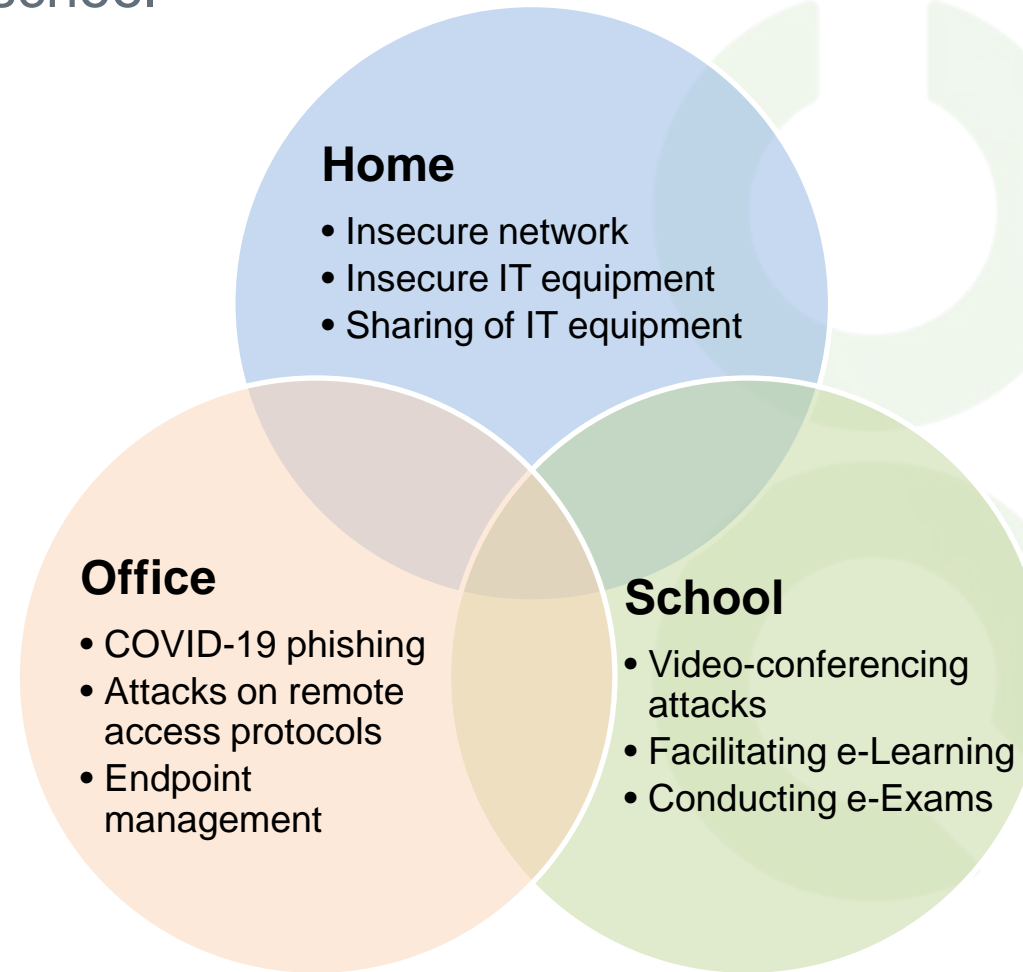
**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



**ISACA**  
Singapore Chapter

# Emerging Challenges from COVID-19

From home to office to school

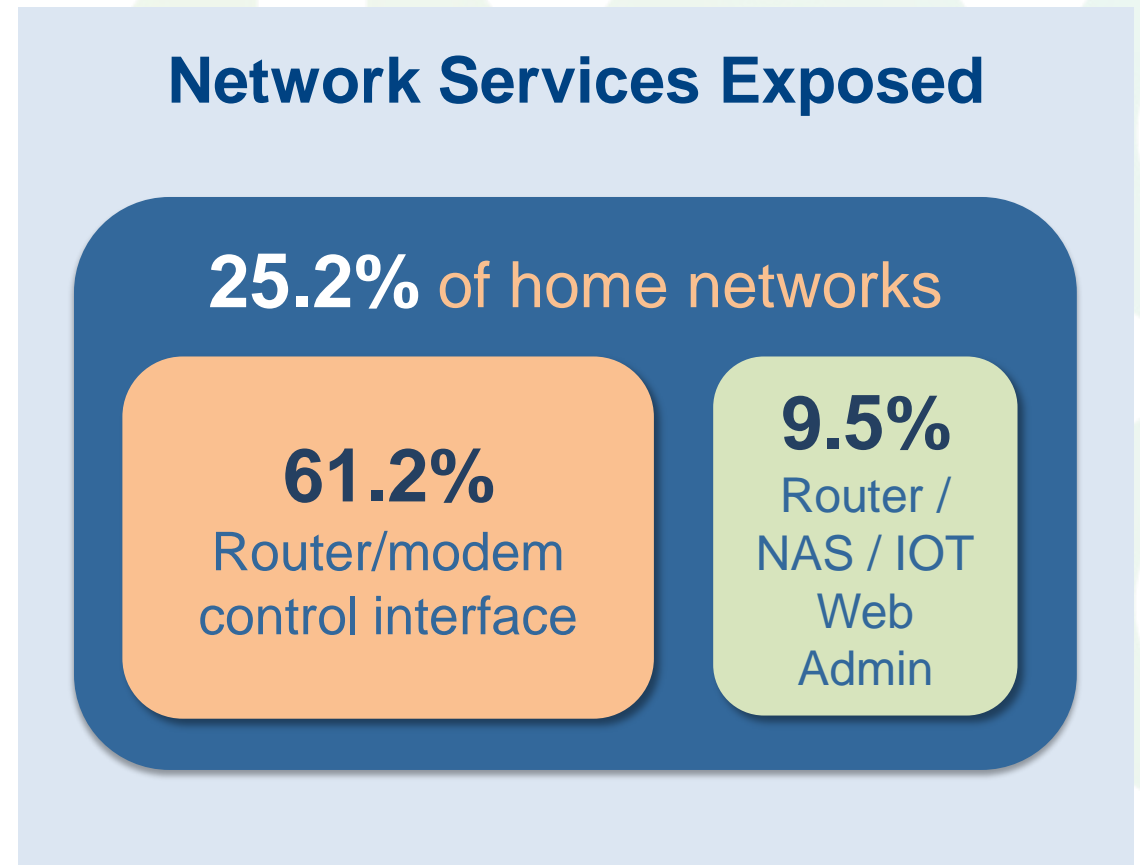
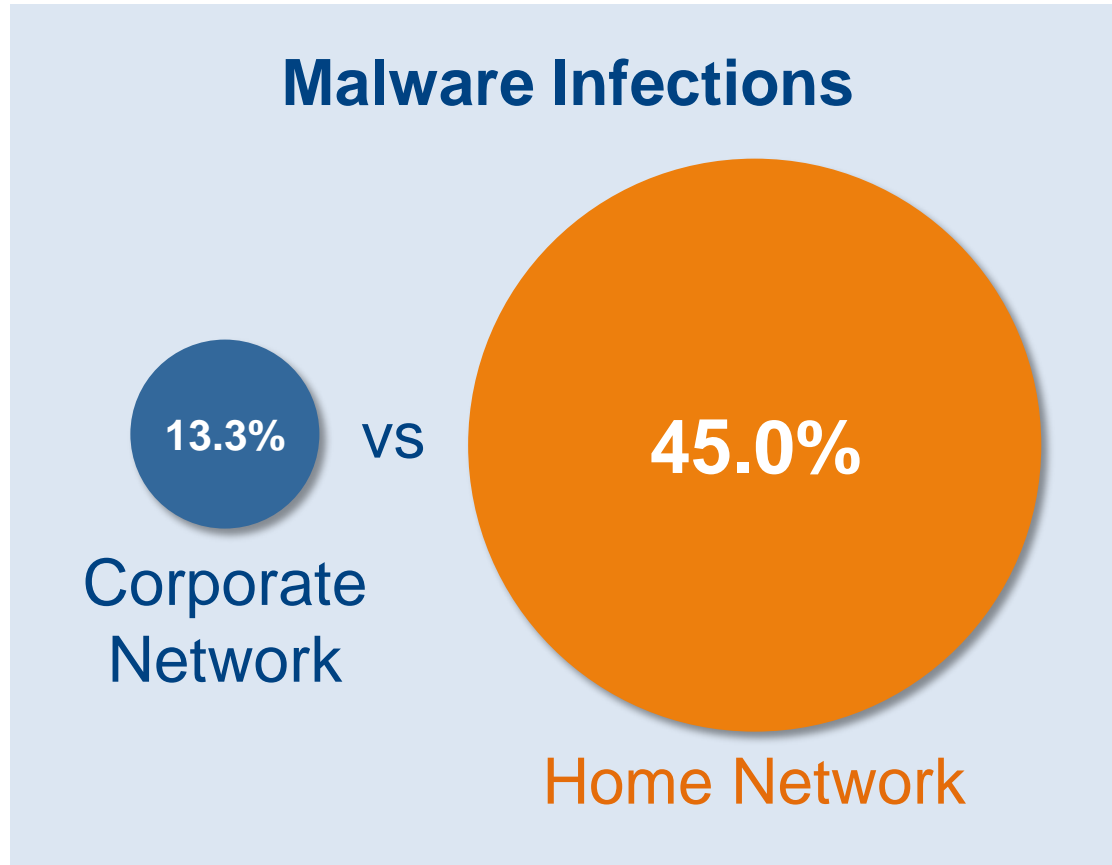


**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

**ISACA**  
Singapore Chapter

# Risks from a Home Network

Observations from a BitSight study conducted in Mar 2020 on 41,000 organizations



Source: <https://www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks>

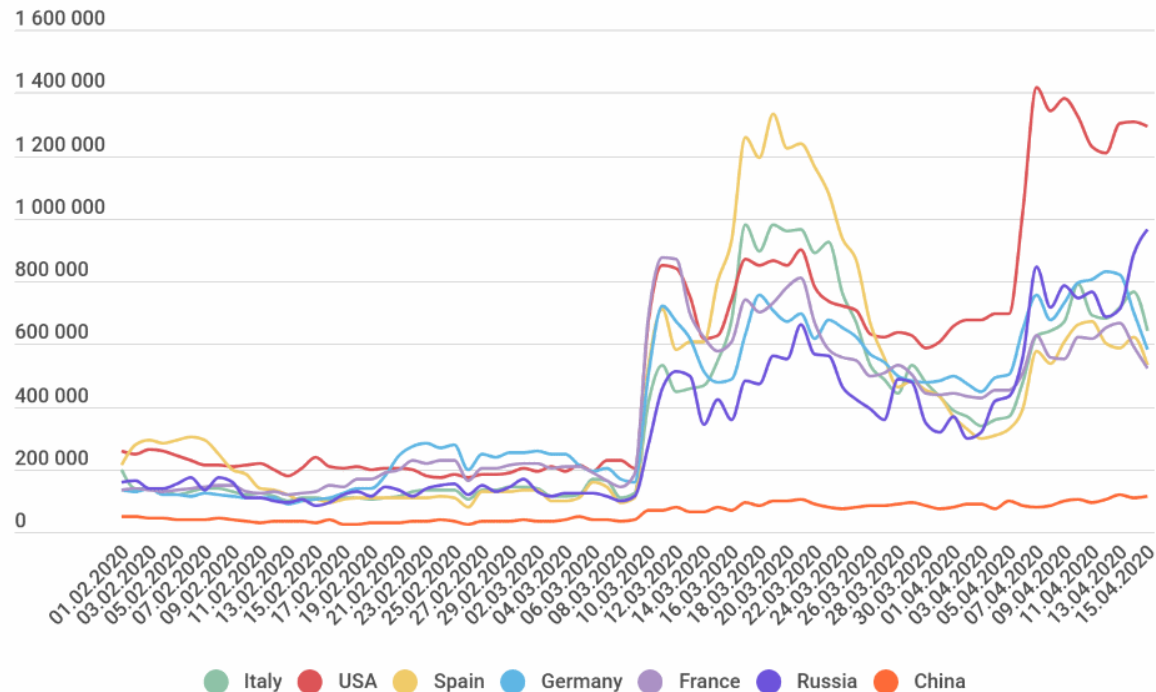


**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

**ISACA**  
Singapore Chapter

# Attacks on Remote Access Protocols

Brute-force attacks on RDP rose sharply



- ▶ Block remote access protocols from Internet
- ▶ Enable 2FA/MFA
- ▶ Enable strong password policy
- ▶ Set and review access permissions
- ▶ Use a VPN gateway
- ▶ Use a Privileged Access Management system
- ▶ Monitor other remote protocols
- ▶ Monitor remote access logs
- ▶ Change default service ports (not recommended)

**Kaspersky: Brute-force RDP attacks between Feb-Apr 2020**

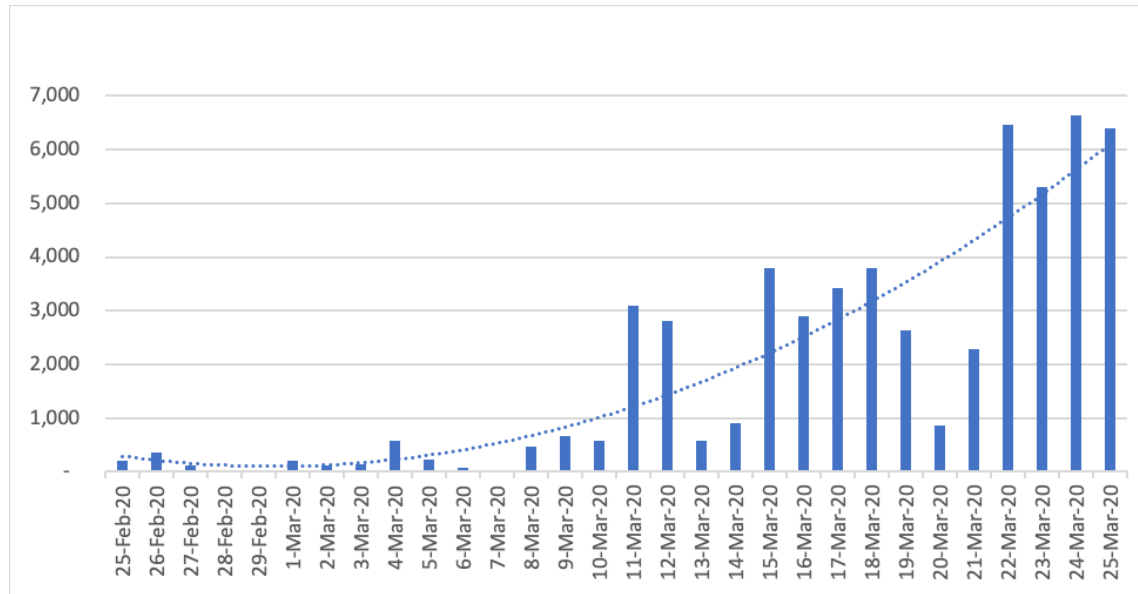


**GTACS 2020**  
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

**ISACA**  
Singapore Chapter

# COVID-19 Related Phishing Attacks

Preying on the human weakness



**MenloSecurity: COVID-19 Phishing Sites Visited**

- ▶ Release regular security advisories
- ▶ Publish educational videos
- ▶ Conduct COVID-19 related phishing drills
- ▶ Use an email-filtering solution
- ▶ Use cyber-intelligence to blacklist related domains
- ▶ Also watch out for Business Email Compromise (BEC) attacks

Video: <https://youtu.be/GOBQzsapNBw>



**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



**ISACA**  
Singapore Chapter

# Remote Access Solutions

Comparing different options of remote working and learning

## VPN

- ▶ Dependent on Internet connectivity
- ▶ Bandwidth considerations
- ▶ Split tunnel gives false sense of security

## VDI

- ▶ Desktop virtualization
- ▶ Hardware independent
- ▶ Resource intensive
- ▶ Not suitable for all apps

## Digital Workspace

- ▶ App virtualization
- ▶ Certificate authentication
- ▶ Endpoint management
- ▶ Device posture check
- ▶ Policy enforcement





# Secure Video Conferencing

The rise of Zoom

- ▶ Prevent “Zoom-bombing” with **enterprise-wide settings**
  - Enable meeting passwords
  - Enable “waiting room”
  - Only allow authenticated users to join
  - Lock the meeting once all participants join
  - Limit screen-sharing to the host only
  - Limit use of Personal Meeting ID (PMI)
- ▶ Update users regularly via security advisories
- ▶ Ensure client is patched to latest



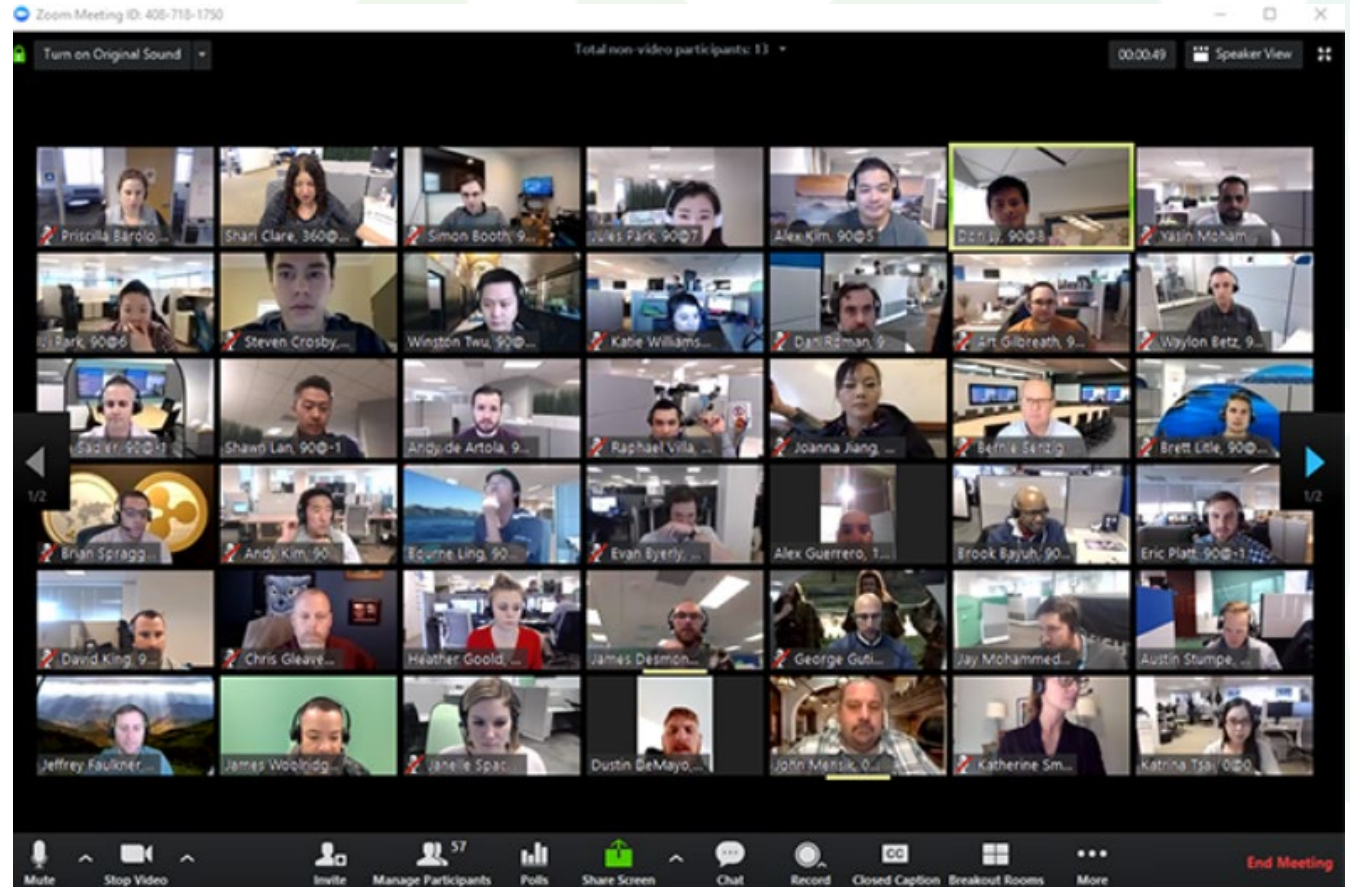
**GTACS 2020**  
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

**ISACA**  
Singapore Chapter

# Conducting e-Exams

Remote proctoring as the new normal

- ▶ What is proctoring
- ▶ Live proctoring vs remote proctoring
- ▶ Auto-proctoring using AI
- ▶ Expensive with setup overheads
- ▶ Alternative using Zoom
  - Quick setup
  - Human invigilators
  - Gallery view
  - Record and review



**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

**ISACA**  
Singapore Chapter

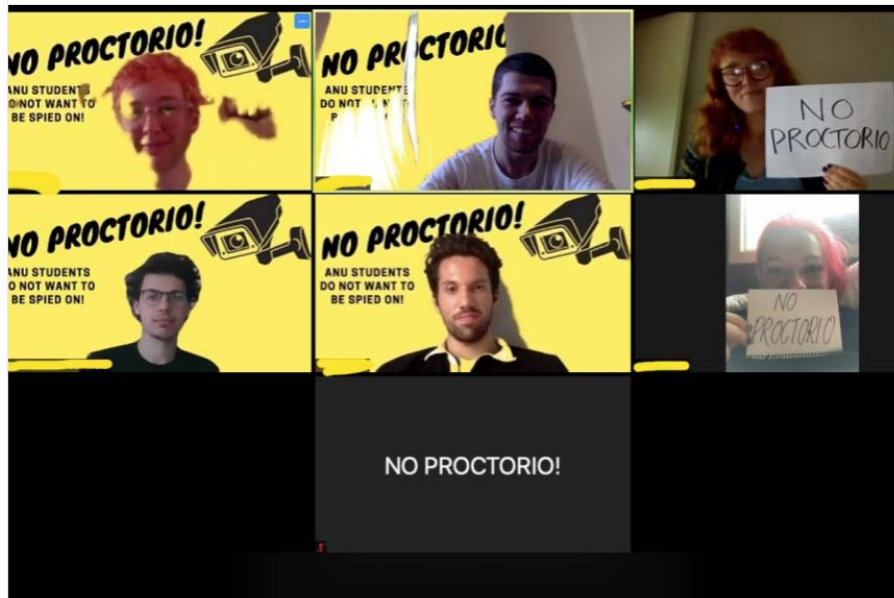
# Issues with e-Exams

To proctor or not?

## ANU to use facial detection software on student computers in response to coronavirus remote exams

By Jake Evans

Posted 20 Apr 2020, updated 22 Apr 2020



- ▶ Most remote proctoring services are SaaS-based
- ▶ Data collection, retention, and sharing
- ▶ Proctoring software = spyware?
- ▶ Dependence on internet connectivity and WIFI
- ▶ Lack of proper personal IT equipment
- ▶ Murphy's Law

## Alternative?



**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



**ISACA**  
Singapore Chapter

# Creating a Lockdown Environment

Beware of security vulnerabilities

**Respondus**  
Assessment Tools for Learning Systems

## LockDown Browser



**Version:** 1.0.7.01

**Your system:** Mac OS X (set by you)

System requirements

Do you need the Windows version?

Are you a computer lab manager?

A screenshot of a web browser showing a GitHub repository page for 'ThreateningYeti'. The browser's address bar shows the URL 'https://github.com/melotic/ThreateningYeti'. The repository name 'ThreateningYeti' is displayed with a 'build passing' status. Below the name, there is a link to 'Download the latest version here'. The main content describes the tool as a bypass for Respondus LockDown Browser, consisting of a DLL injector (YetiLoader) and a DLL (ThreateningYeti). It lists several features such as 'Alt-tab during tests', 'Disabled covering windows', and 'Enabled F1-F12 keys'. A 'Usage' section provides a three-step guide: 1. Download the latest release from a link, 2. Ensure the latest version of Lockdown Browser is running, and 3. Run YetiLoader.exe. The page concludes by stating that YetiLoader will automatically launch Lockdown Browser.



**GTACS 2020**  
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

**ISACA**  
Singapore Chapter

# Takeaways

Applying what you learnt

- ▶ Block common remote access protocols at your Internet gateway
- ▶ Start monitoring remote access logs for potential intrusion
- ▶ Establish an endpoint management strategy for remote machines
- ▶ Conduct COVID-19 related security awareness training for your users
- ▶ Explore alternative remote access solutions
- ▶ Secure your enterprise video conferencing solution through configuration
- ▶ Look into various proctoring solutions and measure the pros and cons



**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



**ISACA**  
Singapore Chapter

# Q&A

## Thank you!



**GTACS 2020**  
GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY



**ISACA**  
Singapore Chapter



# GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY



# ISACA®

Singapore Chapter