Leveraging IT technology for safe distributed workforce

Eric Fan, CEO of UDomain

Agenda

- What is distributed workforce?

- How to work safely in distributed workforce?

- Customer Case Studies
  - Suspending classes without suspending learning（停課不停學）
  - CEO email
  - Online meeting and seminars
  - Online shopping demand
  - Remote Office

- Best Practice for Safe Distributed Workforce

UD

What is distributed workforce?

A distributed workforce is a workforce that reaches beyond the restrictions of a traditional office environment. By installing key **technologies**, distributed companies enable employees **located anywhere** to access all of **the company's resources and software** such as applications, data and e-mail without working within the confines of a physical company-operated facility.
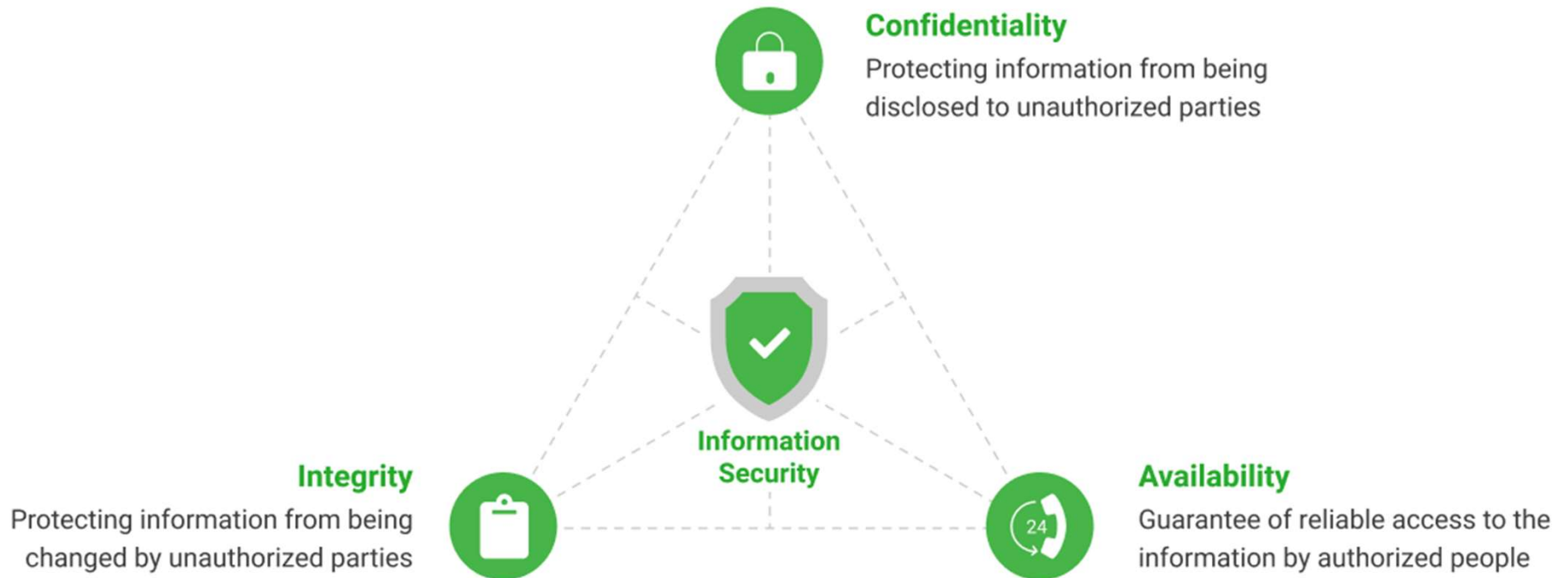
Who led the digital transformation of your company?

A) CEO

B) CTO

C) COVID-19

How to work safely in distributed workforce?

Confidentiality
Protecting information from being disclosed to unauthorized parties

Integrity
Protecting information from being changed by unauthorized parties

Information Security

Availability
Guarantee of reliable access to the information by authorized people

Case 1 - 停課不停學

Background:
During the class suspension period, students moved their learning model to online (watching ETV, Zoom)

無法同步開課 網上學習困難 過半跨境學童受訪者憂引發不公平學習

2020-02-19
來源：香港商報網

　　【香港商報訊】記者王曉蕾報道：新型冠狀病毒疫情嚴重，香港接連實施停課、局部封關及14天強制檢疫等措施，令跨境學童家庭憂慮如香港復課而關口未能開通及14天強制檢疫令未解除，將無法與居港學童同步開課，引發連串問題。

AiTLE x UDomain 網上研討會
跨境學習無疆界 停課不停學

日期：4月15日 （星期三）
時間：10:30am–12:00pm
內客：
－ 面對網站突增流量，教城迅速應變的策略
－ 如何解決跨境學習
－ 跨境平台及安全視像直播
－ 疫情下要注意的網絡陷阱

Case 1 - 停課不停學 (Con'd)

How about the 30,000 cross-boundary students 跨境學童??

Case 1 -停課不停學 (Con'd)

- Security solution in placed
    - Using CDN Network to maintain their availability
    - Encrypted traffic

Case 2 – CEO Email

Background:

- One of the general staff in a listed company receive 'CEO Email' while work from home
- Through this phishing email, hacker injected ransomware to their network and serval database server are encrypted by hacker's password

Case 2 – CEO Email (Con'd)

ProPrivacy | VirusTotal | WHOIS XML API

COVID-19 Malicious Domain Research Hub

Enter any URL related to the Coronavirus below and we will tell you if it has already been flagged as potentially harmful.

Enter URL here...   **CHECK NOW**

AN OPEN DATA PARTNERSHIP

ProPrivacy   **Σ VirusTotal**   **WhoisXML API**
Unified Results!

COVID-19 Malicious Domain Research Hub: Tracking malicious online activity related to the pandemic

99,448 POTENTIAL THREATS DETECTED

With over 350,000 domains analyzed and documented, the COVID-19 Malicious Domain Research Hub aims to become the single largest repository of open data related to malicious online actvity.

https://proprivacy.com/tools/scam-website-checker

Daily Registration of new "Zoom" Domains

cp<r>
CHECK POINT RESEARCH
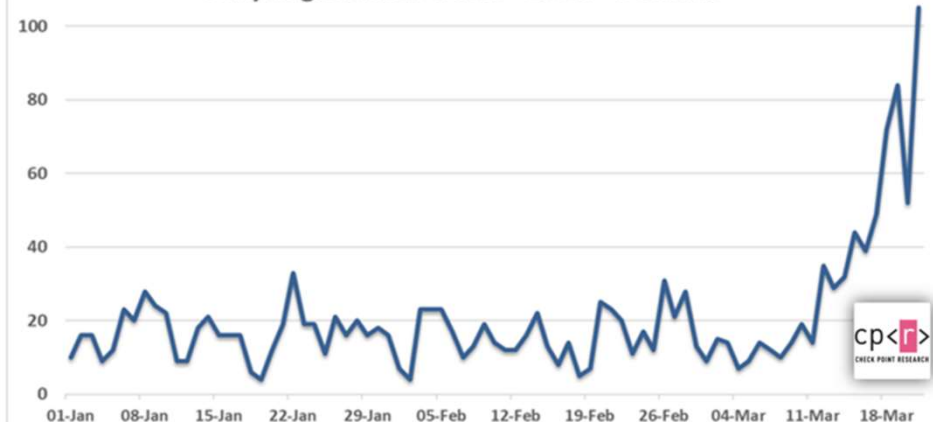
獨家 / 駭客趁疫而入 某銀行被騙走30萬美元

f 分享   🟢 分享   💬 留言   🖨 列印   📥 存新聞

2020-05-07 12:51　經濟日報 記者邱金蘭 / 台北報導　👍 讚 571　分享

Case 2 – CEO Email (Con'd)

- Security solutions in placed:
  - Email Security Solution
  - Full network and server network scanning and patching
  - Backup and tape storage
    - By schedule (bi-weekly full backup, daily incremental backup)
    - 3-2-1 back up practice (Online, Offline, Off-site).
  - Security software and hardware to prevent future attack
    - Cisco OpenDNS
  - Regular penetration test
  - Phishing Email Test & Awareness Training for Employees

UD

Case 3 – Online Meetings and Seminar
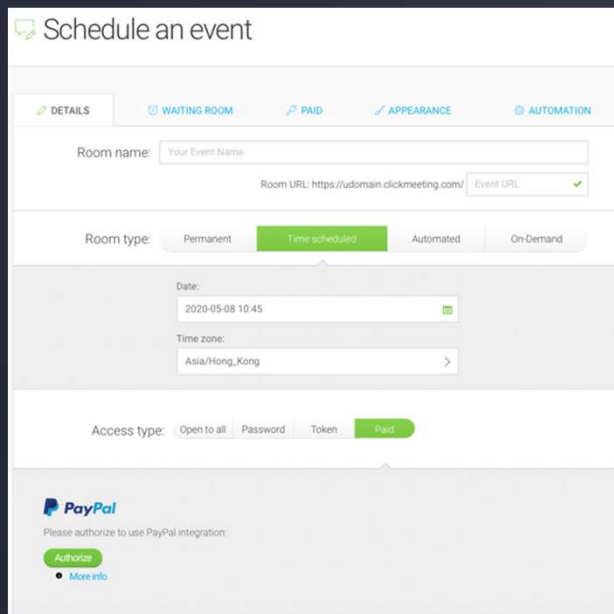
Background

Big4 company have to conduct seminars to 200+ partners while it is not allowed to meet face-to-face. Since the seminar content is confidential and it is important to verify attendee's attendance and identity.
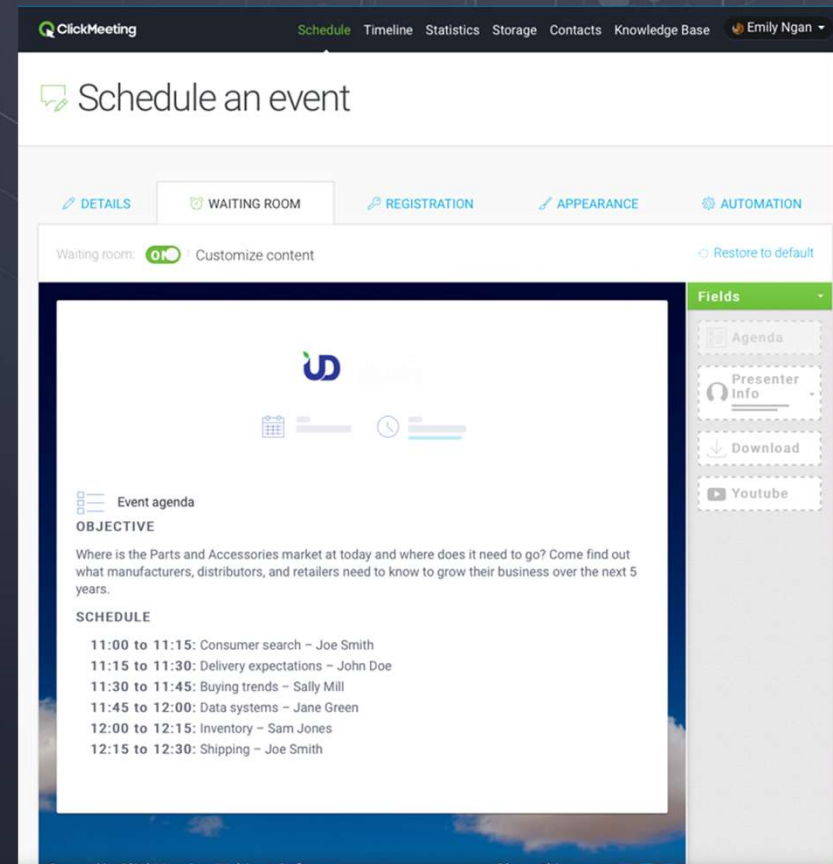
Case 3 – Online Meetings and Seminar (Con'd)

Security solutions in placed:

- Security virtual meeting tools

Virtual Meeting
Practical Guide and Tips

Host like a Pro

- Schedule a rehearsal especially there are multiple host

- Hardwire your internet connection

- Testing on internet connection, audio and video performance, mic and speaker

- Set proper expectations with your audience
  - Recording, time and interaction

- Stream your content to Facebook Live, YouTube or customer Live Stream Services

Advanced Options ⌄

☑ Enable Waiting Room

☐ Enable join before host

☑ Mute participants on entry

☑ Only authenticated users can join: Sign in to Zoom
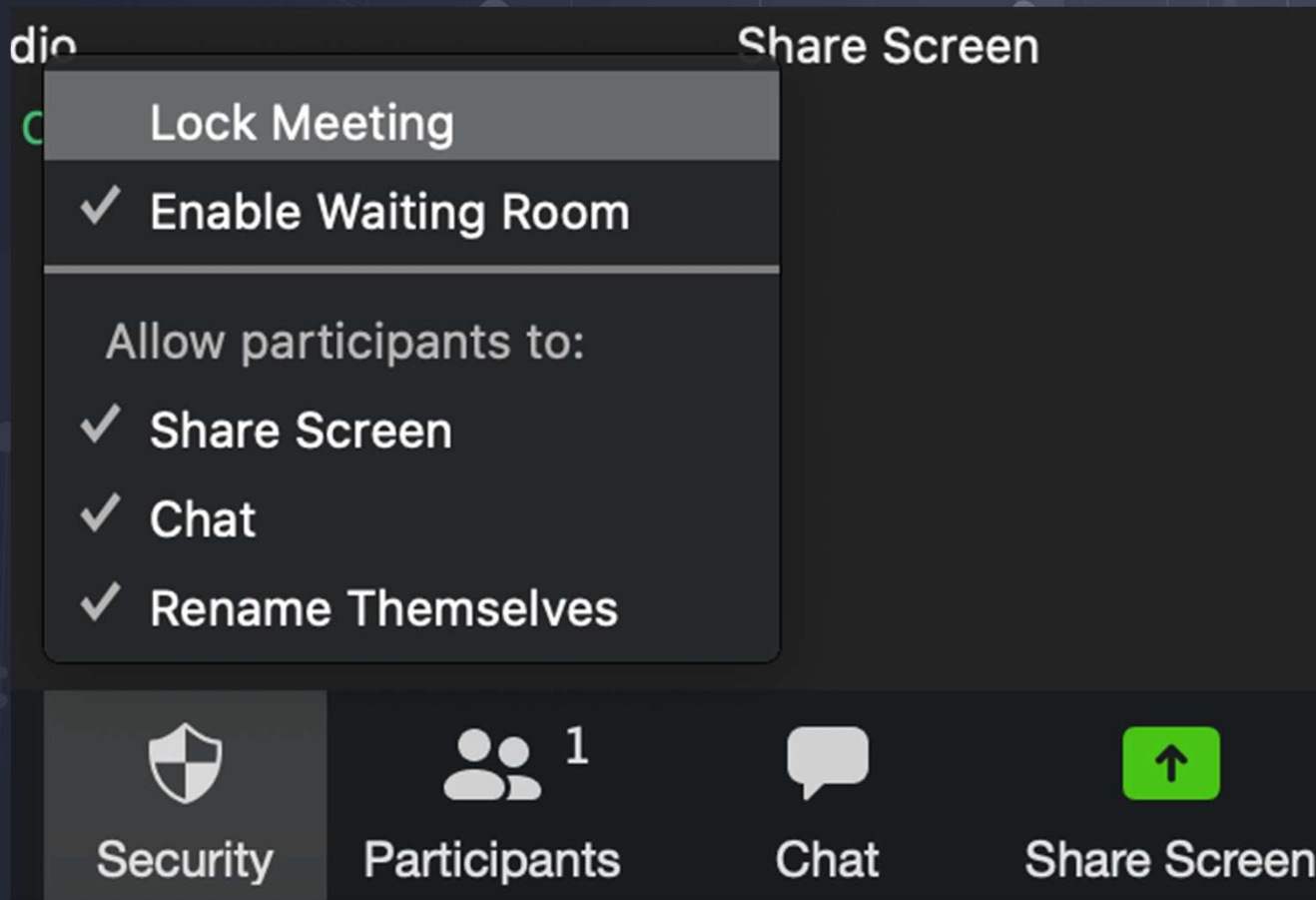
☐ Automatically record meeting on the local compute

Alternative Hosts:

Example:john@company.com;peter@school.edu

1. Enable waiting room to screen every person before joining

2. Mute the participants on entry to avoid voice disturb (like home background noise, music from notebook etc)
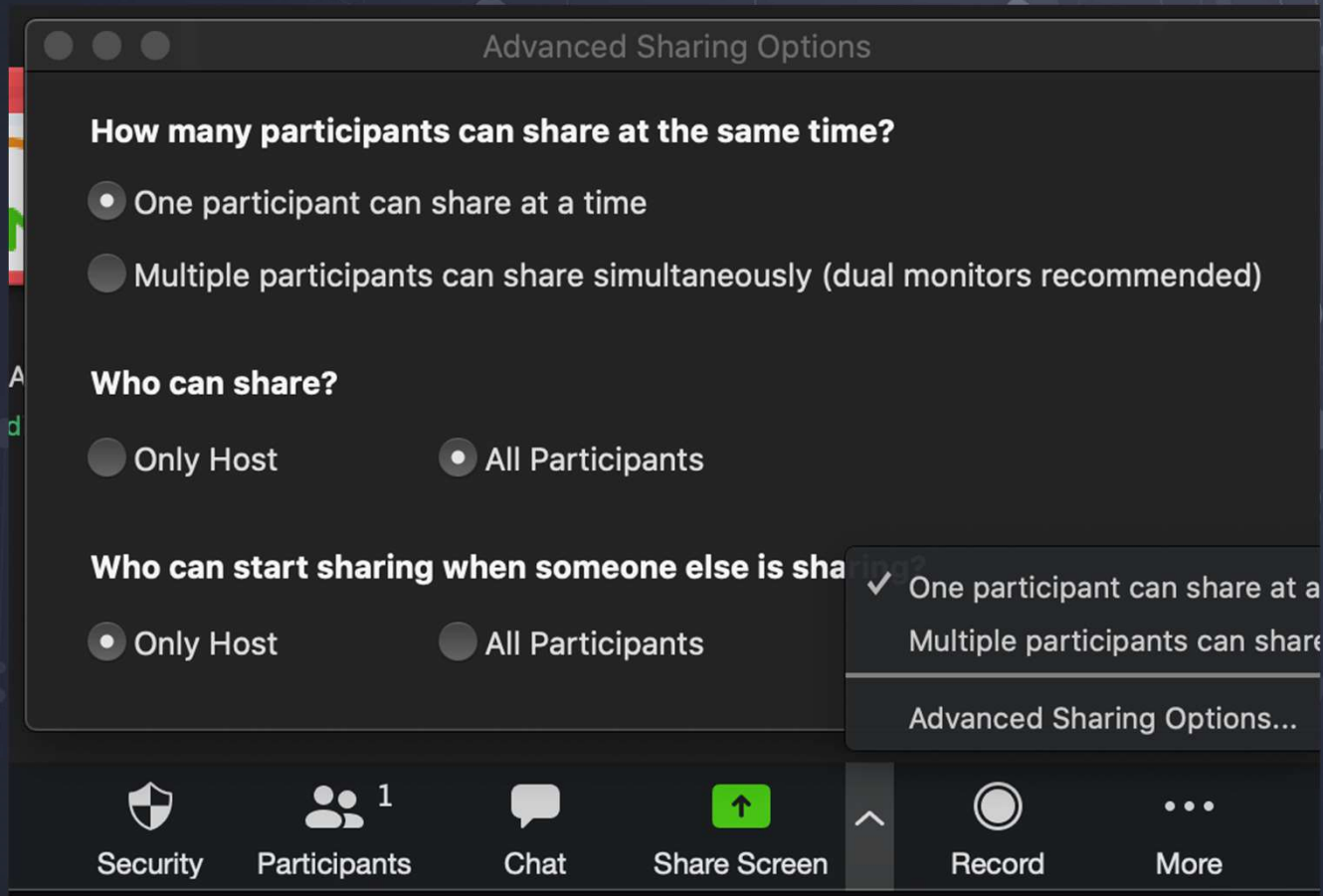
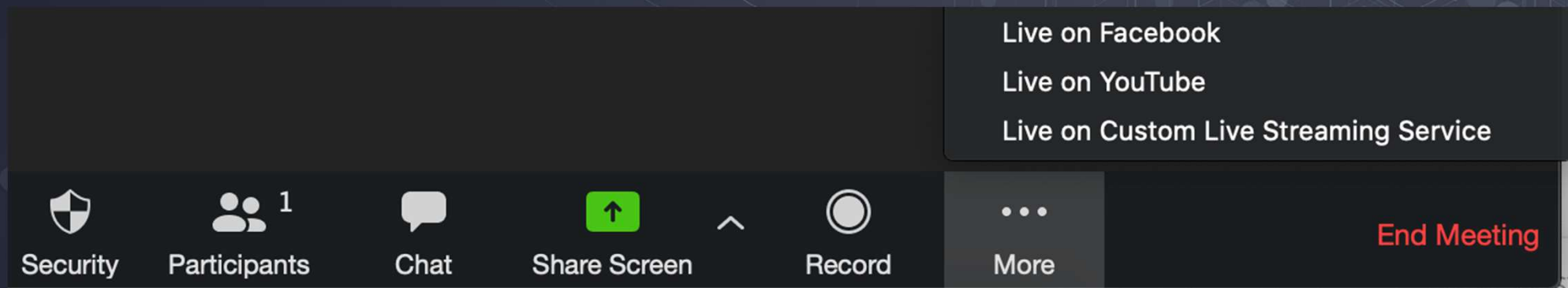1. Disallow participant to chat to avoid unnecessary message broadcast

2. Disallow participant to rename themselves to identify them by email
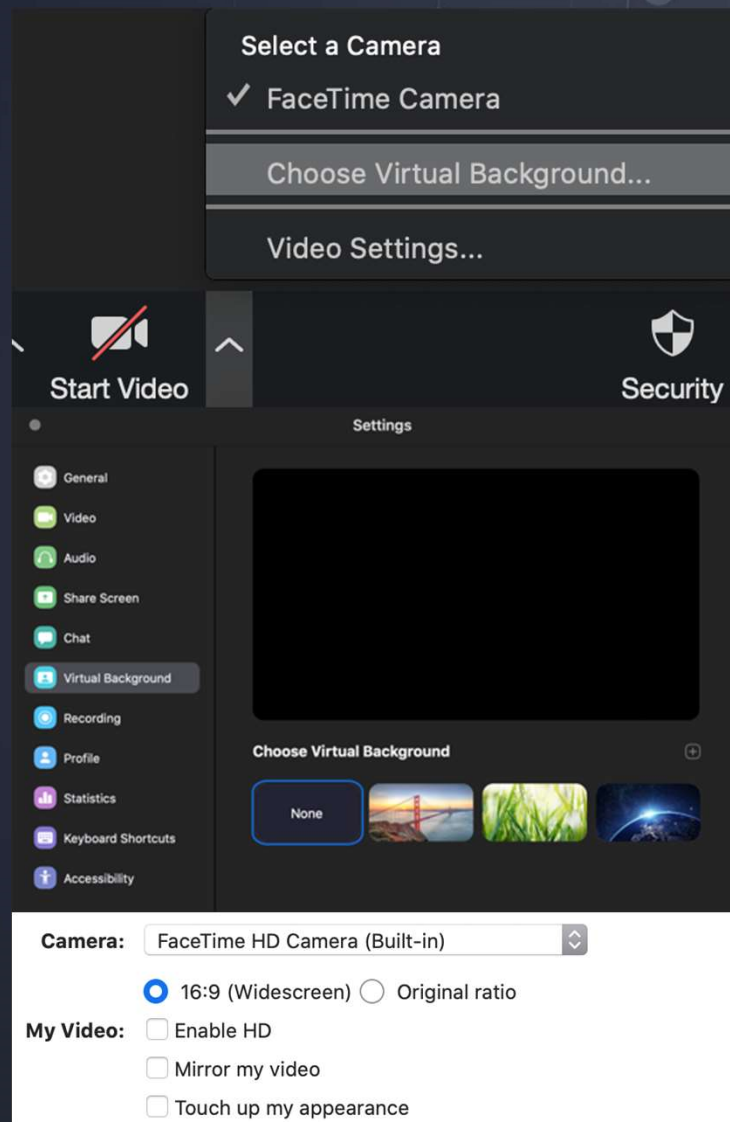
Control the host only to share the screen to avoid unpredicted message share in meeting

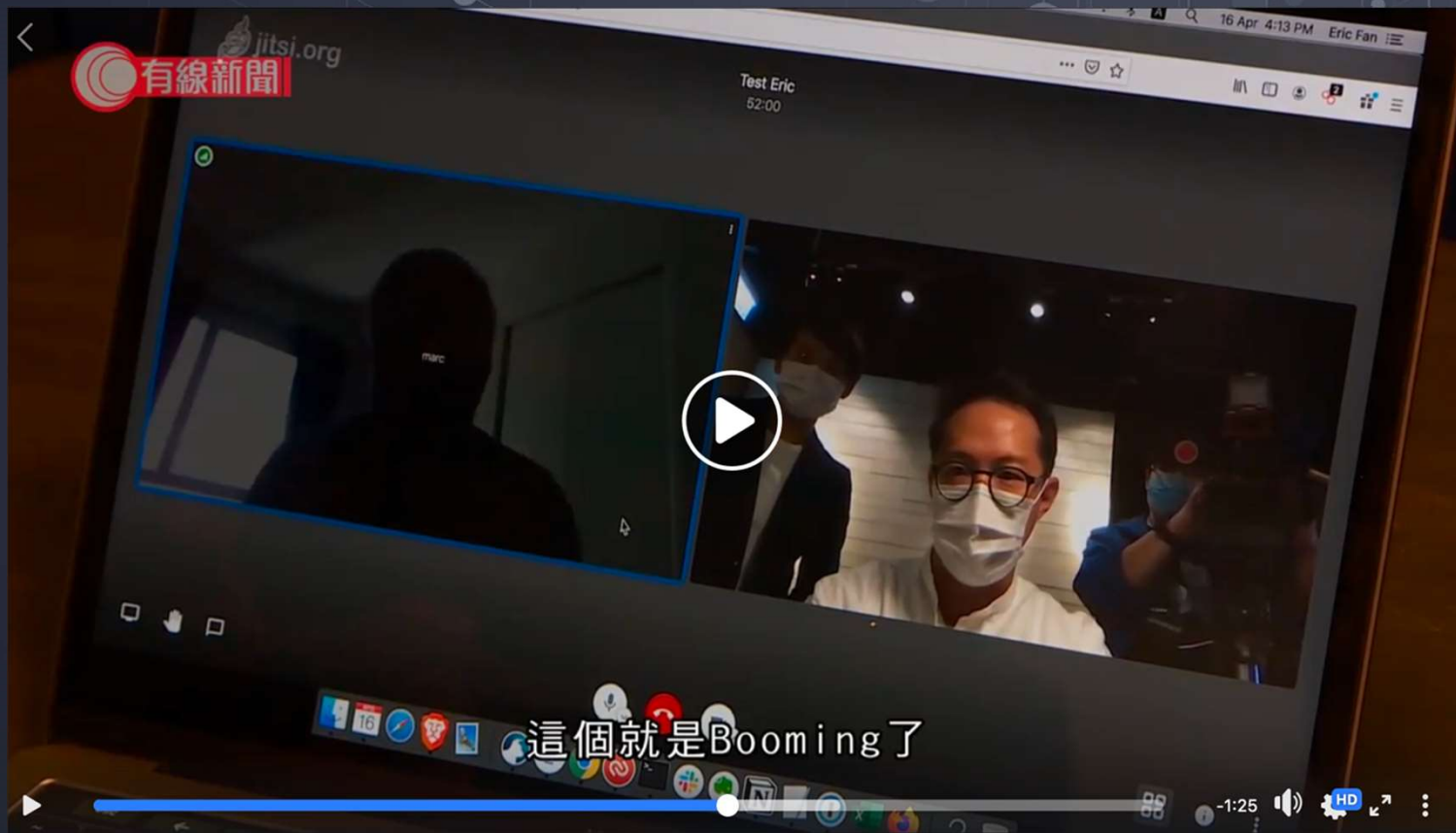# Using social media and live streaming service

Protect your PRIVACY

Set up virtual background before meeting

Bombing: JitSI Meet

	Webex	Microsoft Teams	Google Meet	Jitsi	BigBlueButton	Skype Meet Now	LINE	Zoom
版本	免費版	免費版	G Suite	免費版	免費版	免費版	免費版	免費版
人數	100/原50人	250人	250/原100人	75人	50人為佳	無限制	200人	100/原10人
時間	無/原40分鐘	無限制	無限制	無限制	無限制	無限制	無限制	40分鐘
發起者	需帳號	需帳號	需帳號	免帳號軟體	需帳號	免帳號軟體	需帳號軟體	需帳號軟體
加入者	免帳號軟體	免帳號軟體	免帳號軟體	免帳號軟體	免帳號軟體	免帳號軟體	需帳號軟體	免帳號、裝軟體
加入權限	密碼、主持人接受	網址直接加入	主持人接受	密碼	密碼、主持人接受	網址直接加入	先加入群組	密碼
固定視訊網址	有，也可彈性	無	無	無	有	有（相對不安全）	先加入群組	有，也可彈性
行事曆預約	外掛	付費版功能	Google日曆	外掛	外掛	無	無	外掛
主持人	主持、主講人	由發起者設定	發起者	任何人	發起者	發起者	無	可設定
控制大家焦點	主持人釘選	無	無	跟隨主持人	無	無	無	主持人
靜音他人	主持人	主持人	主持人	任何人	主持人	無	無	主持人
關掉他人視訊	主持人	無	無	無	主持人	無	無	主持人
踢出他人	主持人	主持人	主持人	任何人	主持人	無	無	主持人
共享畫面	一次一人	一次一人	一次一人	多人可同時共享（看網路速度）	一次一人	一次一人	一次一人	一次一人

- https://www.playpcesor.com/2020/04/webex-teams-meet-jitsi-8.html

Virtual meeting tips

範健文 ⊙April 2, 2020

【范健文】在Zoom為子女開生日會遇不速之客？教你應對五式

【Zoom危機】 專家教網絡會議6大tips 要避免經WhatsApp 傳送會議連結

更新時間 (HKT): 2020.04.09 00:06

范健文 Eric
網絡安全專家
網頁寄存供應商UDomain CEO

例如「googleclassroom.hk」

1:35   4:53

Case 4 – Online Shopping Demand

Background

Online shopping and website demand had increased rapidly during COVID-19 and 'Social Distancing Regulations'

Case 4 – Online Shopping Demand (Con'd)

- Secure solution in placed
  - Managed Secure Cloud Hosting
  - Queneing system and email broadcast
  - Penetration test and vulnerability scanning
  - Stress test

Case 5 – Remote Office

Background

- HKSME not ready for Work from Home? No secure solution, using Remote Desktop/Teamviewer?

- HKSME File Sharing between HK and China Office become headache

- Our client's employees were unable to go to office as usual for the disease outbreak, yet work-from-home was not feasible as all the files were stored in the company's server.

Case 5 – Remote Office (Con'd)

- Secure solutions in placed:
  - Upgrade and Set up VPN connection
    - set up 20 VPN accounts through the client's firewall remotely with 2 factors authentication
    - File, database and email servers were set up to enable employees accessing data and information in a secure environment.
  - Video Conference Training
    Meeting client and its employees through video conference for a tutorial on the installation and use of VPN accounts

Above set up and training completed within one day without any physical interaction

Secure Authentication

- Cloud Storage Solution
  - Single Sign On, 2 Factors Authentication
  - Google Drive, Dropbox, OwnCloud

https://authy.com
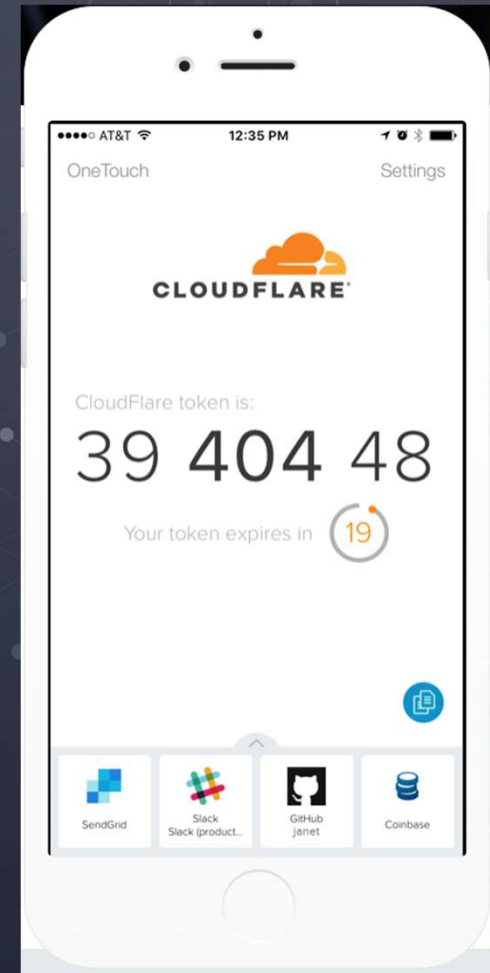
Best Practice of Safe Distributed Workforce
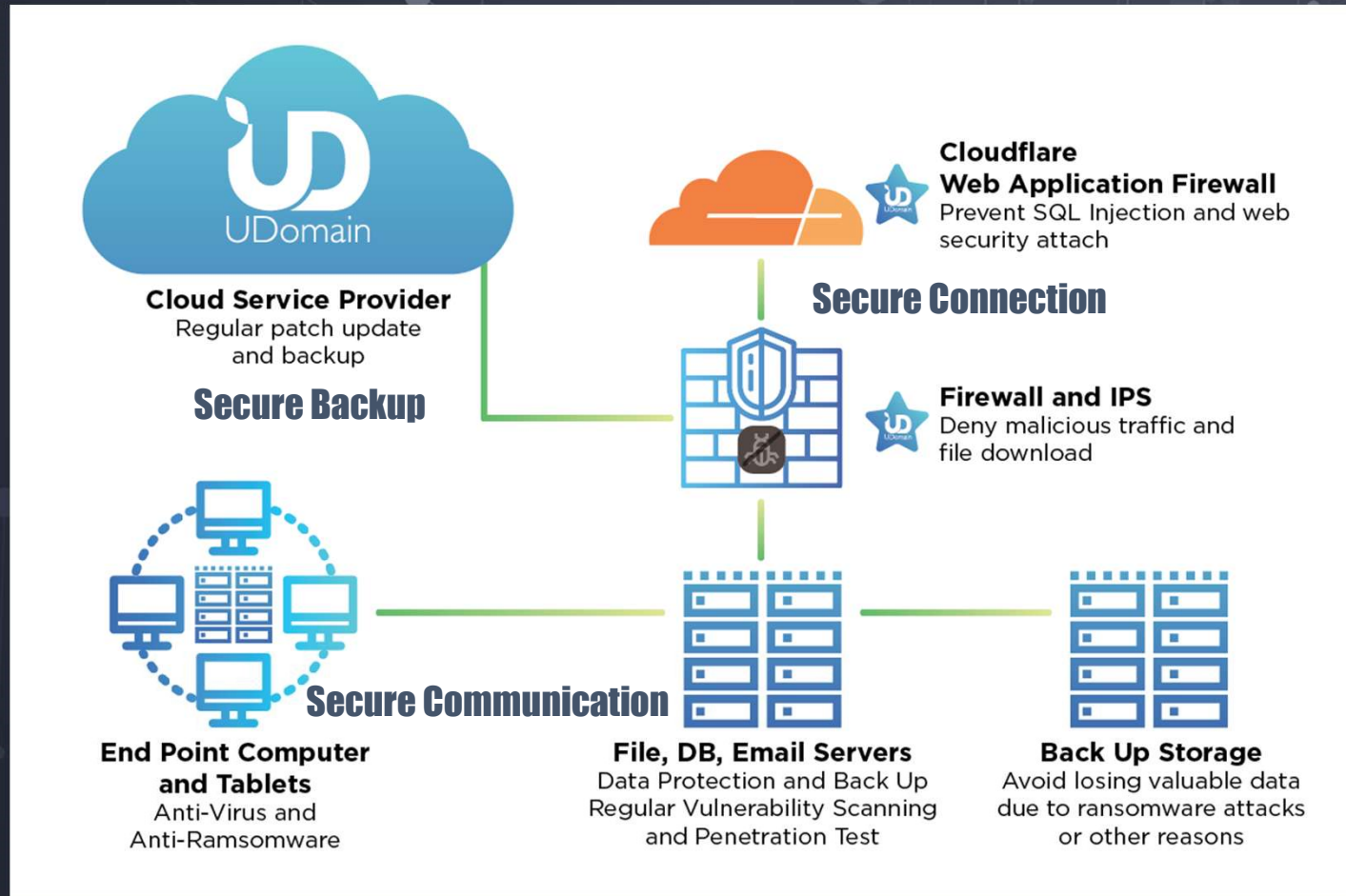
D-Biz Programme

網絡遙距管理方案　　網上會議安全方案　　雲端託管安全方案　　Google雲端整合方案

List of free trial software and tools

- https://www.bleepingcomputer.com/news/software/list-of-free-software-and-services-during-coronavirus-outbreak/

Thank You!

Appendix

Modern Worker Classification

Fixed / Static

Traditional office tasks ranging from office support, onsite service
Admin, Receptionist

Telecommuter

Staff that work at home or satellite office
Branch sales rep, data center operator, call center operator

Extremely Mobile

Perform both individual and group work and work from anywhere
Sales and BD, Top Management

Internally Mobile

Alternate between individual and group work
Finance, Engineer, Programmer, Marketing

Digital transformation pros & cons

PROS

MAKES YOUR BUSINESS MORE COMPETITIVE

MAKES YOUR EMPLOYEES MORE PRODUCTIVE

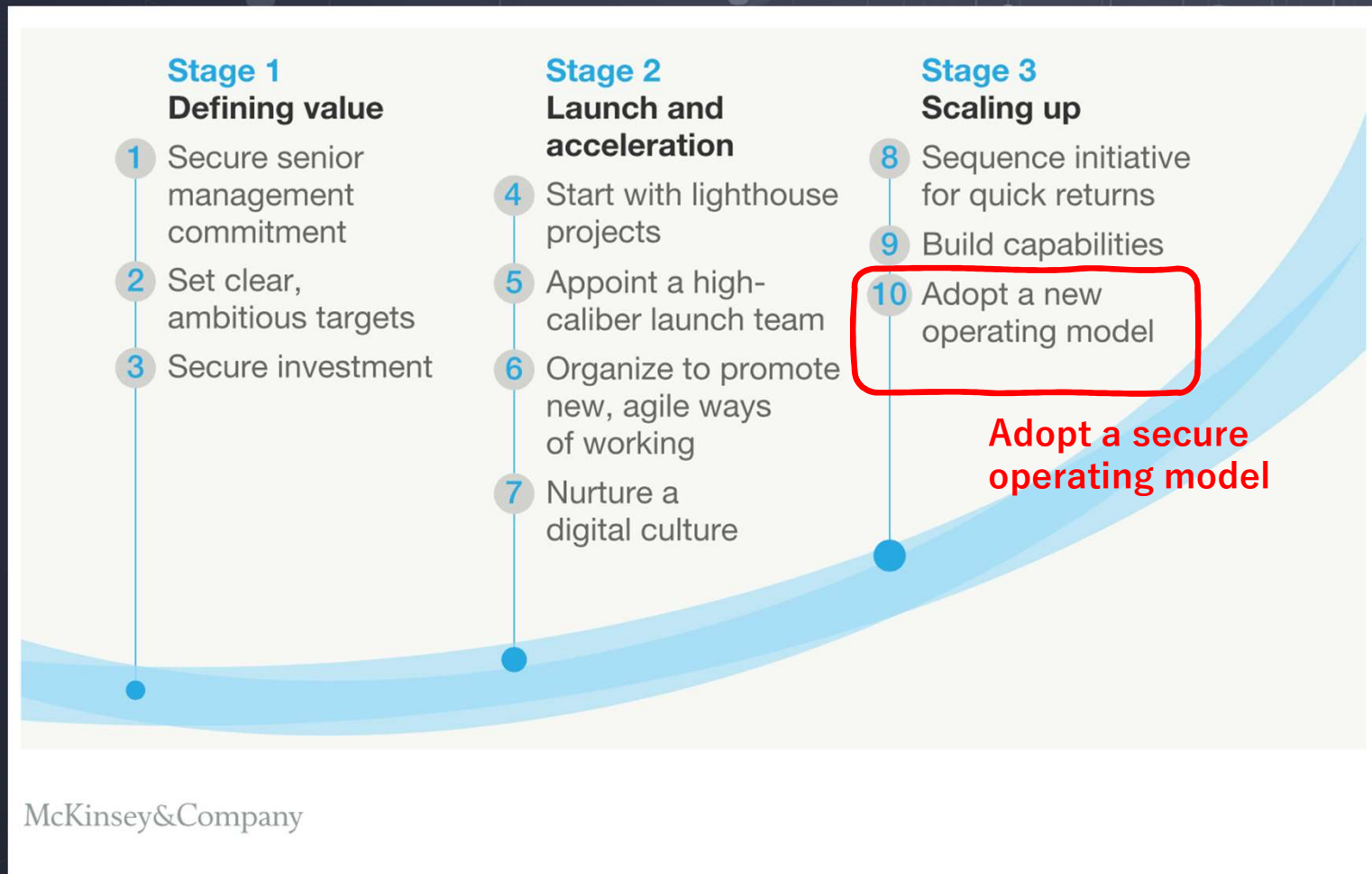**ALLOWS YOU TO PROVIDE A BETTER CUSTOMER EXPERIENCE**

CONS

EFFECTIVE IMPLEMENTATION OF NEW TECHNOLOGIES TAKES TIME

OPERATIONAL SECURITY IMPLEMENTATION

Top 10 guiding principle of a digital transformation

Stage 1
Defining value

1 Secure senior management commitment

2 Set clear, ambitious targets

3 Secure investment

Stage 2
Launch and acceleration

4 Start with lighthouse projects

5 Appoint a high-caliber launch team

6 Organize to promote new, agile ways of working

7 Nurture a digital culture

Stage 3
Scaling up

8 Sequence initiative for quick returns

9 Build capabilities

10 Adopt a new operating model

Adopt a secure operating model

McKinsey&Company

Cyber Security Assessment

Vulnerability Scanning

- Scanning the system using professional tool
- Generate scanning report

Black Box Testing

- Know nothing about the system, like a normal user
- Close to the real hacker
- Might only find minor issue

Grey Box Testing

- Some level of knowledge on the system
- Most common approach to do penetration test
- A more accurate result

White Box Testing

- Know everything on the system, including the source code
- We will provide this in the next phase

Report & Recommendations

Debriefing meeting

Executive Summary

Testing Methodologies

Proof of Concept

Impact and Severity

Findings Details

Recommendations
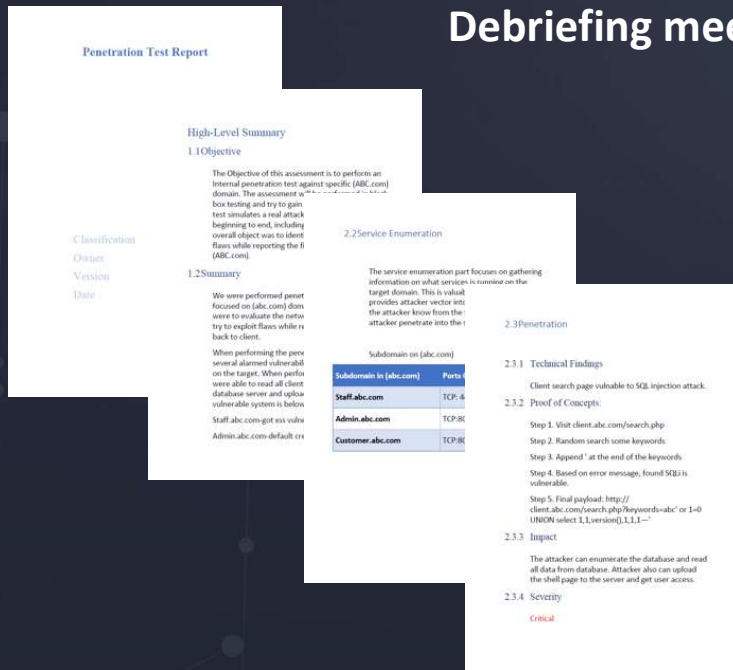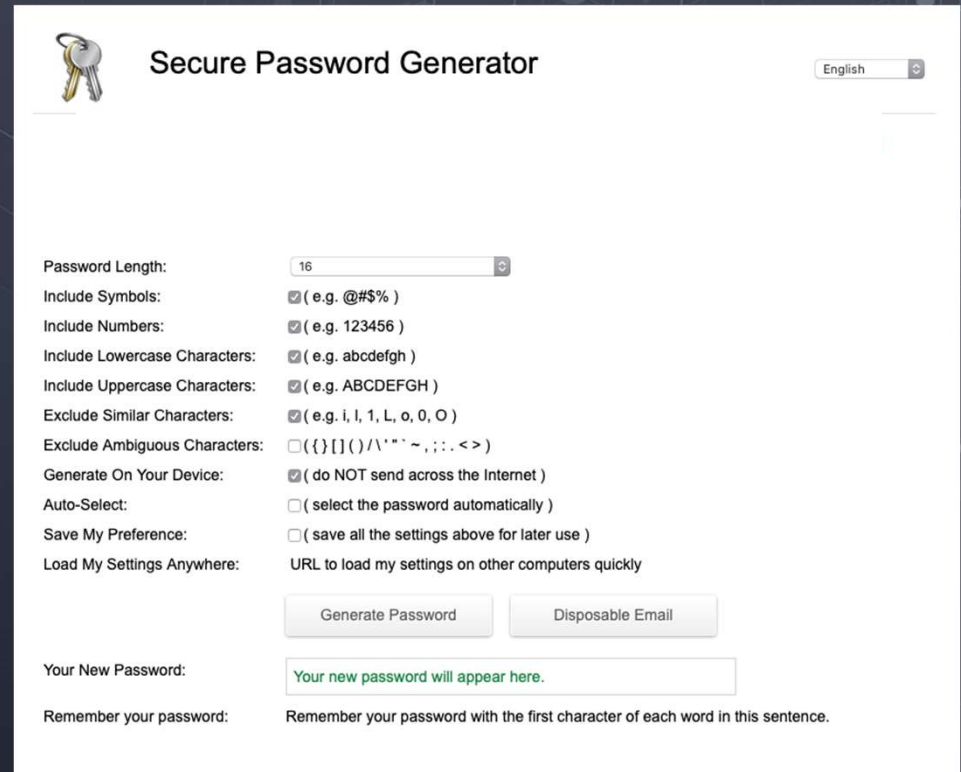
Availability

- Backup and tape storage
  - By schedule (bi-weekly full backup, daily incremental backup)
  - 3-2-1 back up practice (Online, Offline, Off-site)
- Access Control
  - Need-to-Know, Least Privilege and Segregation-of-Duties principles.
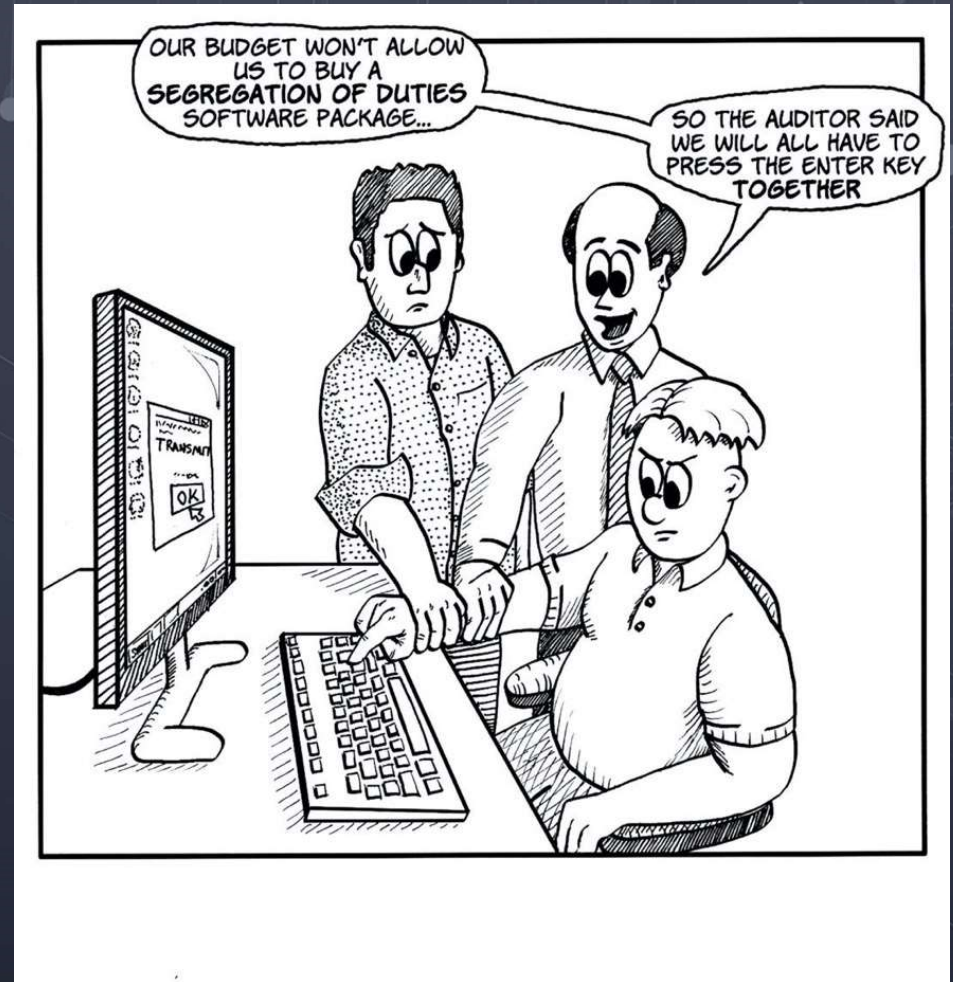
Confidentiality

- Encryption
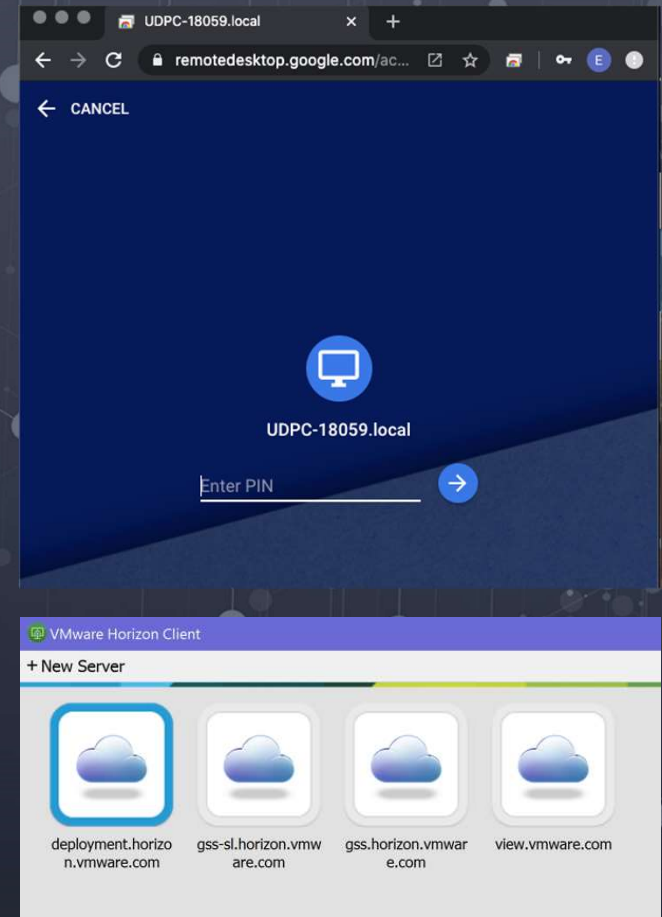 - Network
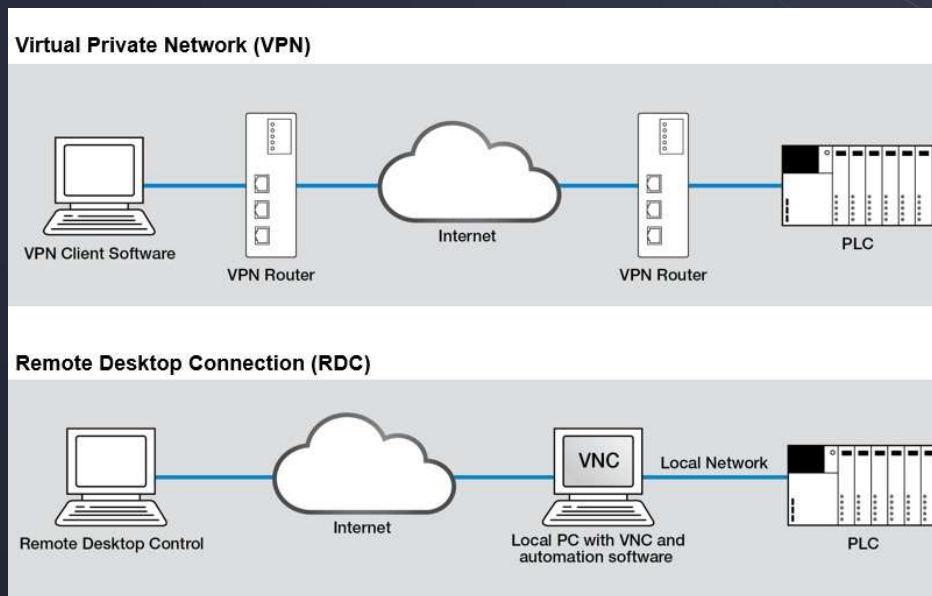 - Data
- Password Policy

Integrity

- Remote patching and reboot
- Authentication and Access control
- Data leakage
- Audit and Review
  - Vulnerability Scanning, Patching

Secure Connection

- Remote Desktop / VDI Demo
  - How to establish secure network connection

Secure Communications

- Email
  - 2 Factor Authenticator, Google Authenticator
  - China email
- Phone
  - Softphone
  - Unified Communication: IM, Chatbot
- Virtual Meeting
  - Training, Live Streaming
  - Document Sharing

Secure Cloud Storage / Remote File Server

Other Cloud Storage Service

- Risky unencrypted transaction
- Blocked in Mainland China
- Unbranded and generic sharing URL
- Limited number of users and limited features

UD Cloud Storage Service

- Safe 256 bit encrypted transaction on all plans
- Comprehensive connectivity to China and the world
- Sharing URL customized for your domain to present a more professional image
- Unlimited number of users and storage can be freely allocated

Supplementary / Key Take Away

- Staff handbook – Use of Computer Device Policy
  - Secure Communications
    - Email, Phone, Instant Message
  - Secure Connection
    - VPN, Remote Desktop, VDI
  - Secure Back Up
    - Encrypted

UD