SCOTTSDALE INSTITUTE

COLLABORATION • EDUCATION • NETWORKING

You may contact us at
scottsdale@scottsdaleinstitute.org / (763) 710-7089.

Managing Your Expanding Remote Workforce During COVID-19 and Thereafter

April 15, 2020

Impact advisors

Agenda

- Introductions
- Problem Statement
- Infrastructure Considerations
- Security Considerations
- Questions

Introductions

Erik Gerard, Principal Advisor and VCTO

Mr. Gerard is a seasoned IT leader with almost twenty-five years of experience working in technology, including 15 years in management roles. He has a deep background in high availability, large-scale technology in healthcare. He is ITIL certified and skilled at translating business needs into innovative technology solutions that provide a competitive advantage.

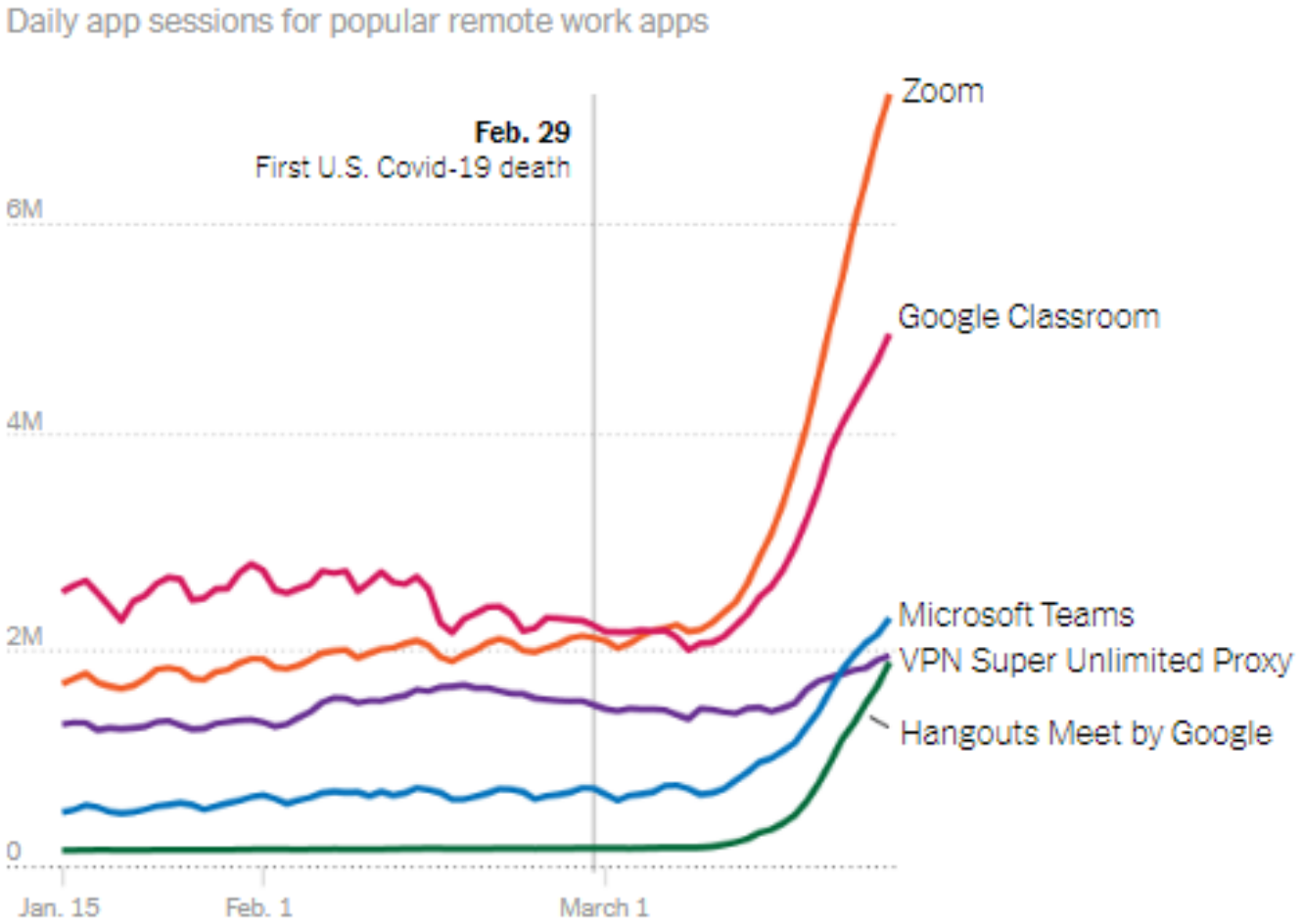
Shefali Mookencherry, Principal Advisor and VCISO

Ms. Mookencherry is a Subject Matter Expert in GDPR, HIPAA, ISO 27000 certification readiness, healthcare information privacy and security, cybersecurity, disaster recovery, health policy and strategy, revenue cycle, reimbursement, Promoting Interoperability (PI), MACRA/MIPS/APMs/QPP and compliance. Shefali has over 25 years of healthcare experience with 9 of those years in senior management positions.

Problem Statement: Managing an Expanding Remote Workforce

- How are employees collaborating and communicating to remain effective and efficient?
- Are these tools and workflows secure, scalable and manageable?
- Clinical vs. non-clinical may be approached differently
- Which functions could continue to operate remotely successfully in the long term?

Trending Teleconferencing Tools



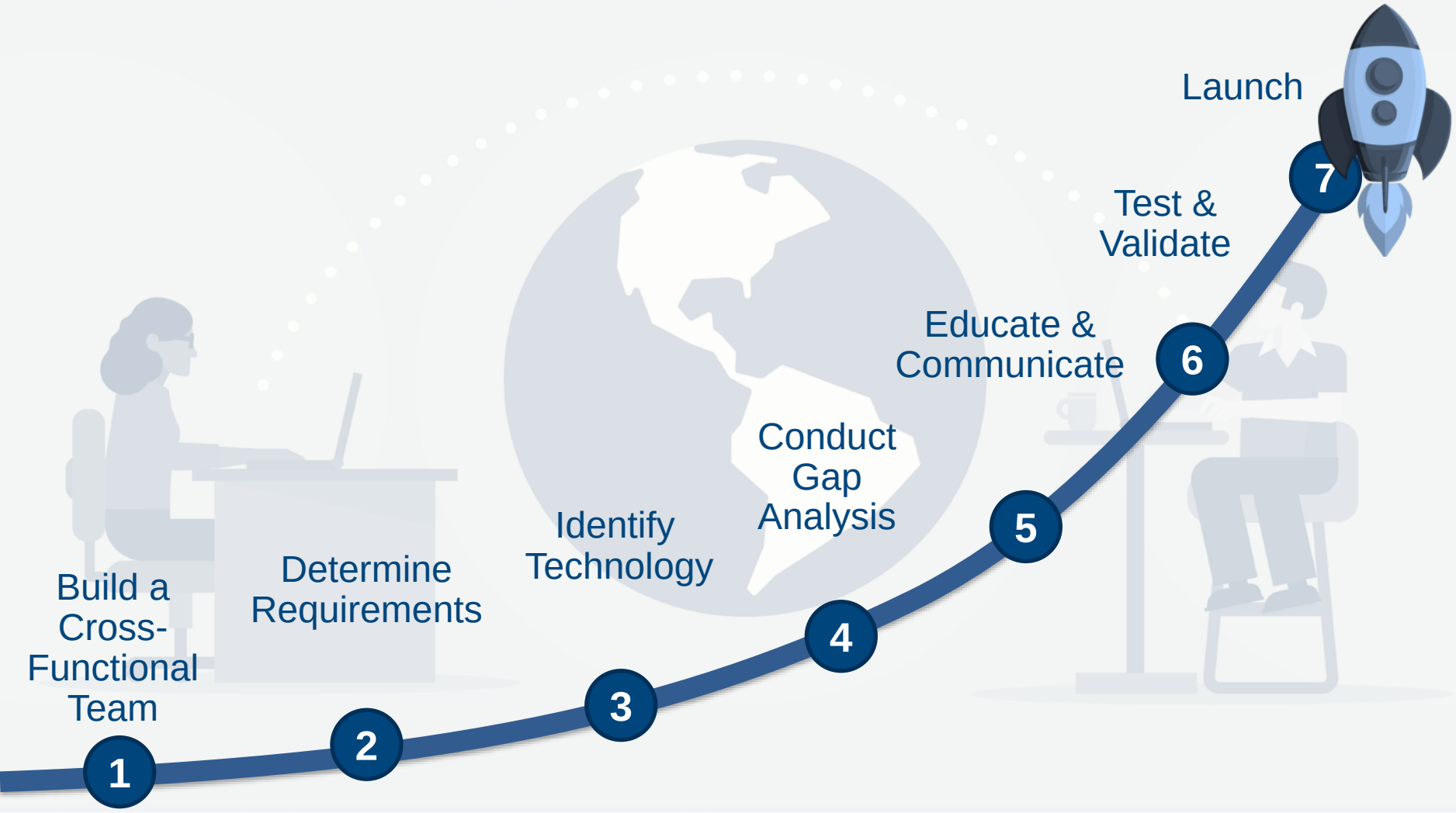
Infrastructure Considerations

- What tools are they using?
  - For collaboration?
  - For application access?
- Can you accommodate the increased load?
  - Either in your data enter or in the cloud?
  - Is there network bandwidth to support the additional volume?
- Is the service desk trained to support additional tools and users?

For Resources Already Working Remotely…

- What applications are they using – cloud based?
- Are the applications HIPAA compliant?
- How are they authenticating – 2Factor?
- What devices are being used and how are these devices managed? Are the devices secured?
- Is the connection method secure? End-to-end encrypted?
- Are policies in place to govern use?
- How are policies being communicated?
- How are you preventing misuse?
- Are remote employees printing and/or scanning PHI?
- Is there a policy that addresses shredding PHI at home?

Scaling Remote Access Capabilities

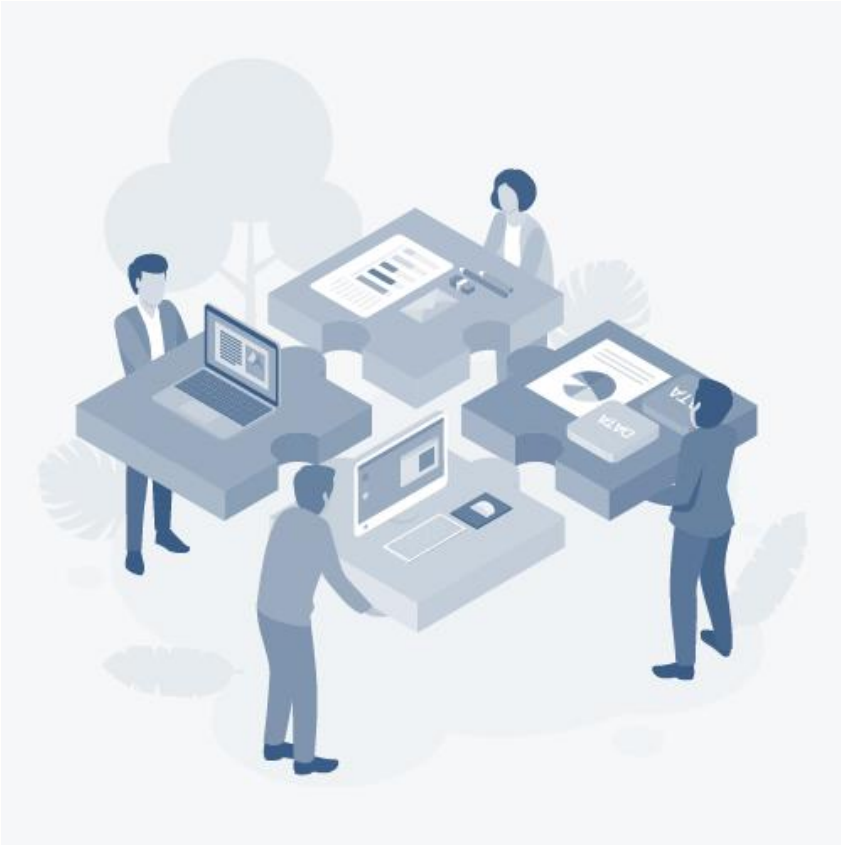


Security Considerations

- Be an active participant in the COVID-19 Command Center
  - CISO or designated information security staff
- Develop and implement:
  - Remote Work Policy
  - Telehealth Policy
  - Video-Conferencing Policy
  - IT Security Data Loss Protection (DLP) Tool Policy
- Establish and communicate IT security standards for telehealth
  - Internal IT security
  - Providers and patients
  - Researchers and educational purposes
  - Business associates, partners, vendors, etc.
- Perform telehealth solutions vendor security risk assessments
  - e.g., COVID-19 Rapid Test vendor
- Review Disaster Recovery and Business Continuity Plans

Build a Cross-Functional Team

- IT Security
  - To assess risk and security of the tools and processes selected
- IT Infrastructure
  - To ensure solutions are accessible by users/customers, and have the scale and capacity to support anticipated workloads
- Leadership Team
- Clinical Team
- Back-office Team
  - Revenue Cycle, Marketing, Scheduling, Accounts Receivable, etc.



Determine Requirements

- Collaboration Requirements
  - Internal and/or external attendees?
  - Maximum number of attendees?
  - Audio (dial-in or web browser or within an app)?
  - Screen sharing?
  - Video?
  - Recording?
- Application Access Requirements
  - Individual applications or full desktop?
  - How are these being delivered normally?
- Identify Internal Users Who Will Leverage These Toolsets
  - May determine bandwidth requirements
- Determine Training Requirements & Communication Plan

Security Considerations

- Review and modify (as needed) organization's website security
- Stay up to date on COVID-19 cyber scams and security alerts
  - WHO and CDC phishing emails
  - Homeland Security Alerts and Bulletins
  - Office of Civil Rights (OCR) Public Notifications
  - OCR Security listserv
- Develop plan to prioritize and implement mitigation activities for COVID-19 related cyber scams
- Determine workflow for COVID-19 test results reporting to HHS
  - What security controls are in place for securely reporting PHI?
- Update access provisioning and de-provisioning procedures
  - Furloughed employees

Identify Technology

Leverage & expand existing technology

Expand capacity of data center or cloud?

Network bandwidth?

Explore cloud-based collaboration options

WebEx, Skype, MS Teams, GoToMeeting, Zoom, Google Meets, etc.?

Determine application access

Virtual application delivery?

Virtual desktop?

Conduct Gap Analysis

- Compare Requirements vs. Capabilities
- Identify Gaps
- Determine Mitigation Strategies
- Develop Plans

Educate and Communicate

- Instructions on how tools are installed, launched, used, etc.
  - Basic and advanced functions
  - Post instructions to intranet and external website
- IT security standards for telehealth across all functions and specialties
- New and/or modify existing consents for telehealth workflow
- Education for staff on phishing – cyber scams are increasing

Test & Validate

Test Basic Functionality

Test Advanced Functionality

Test Users

Test Service Desk

Stress Test
Engage multiple users concurrently in a scheduled test of capacity

Adjust Bandwidth or Configuration Accordingly

Launch

Verify:

- Testing complete
- Documentation in place
- Training complete

- Support services informed and ready
- Update intranet and external website

Communicate!

Long-term Considerations

- What are the potential savings of remote workers?
  - Office space and furnishings, electricity, parking, etc.
  - Access to resources outside of immediate geographical area (better skills, less expensive)
- Which remote teams worked successfully and why? Which did not?
- What adjustments are necessary to make remote teams successful in the future (culture, workflow)?

Recommended Actions

- Track costs for COVID-19 telehealth security
  - Bandwidth, laptops, iPhones, outsourcing resources, etc.
- Respond to Relief Fund Programs
  - FCC
  - FEMA
  - CARES Act
- Post COVID-19, remote workforce needs will likely remain…
  - Evaluate security controls in place and determine modifications
  - Modify IT security standards for telehealth, as applicable
  - Review IT security regulatory requirements
  - Determine if tactical deployments are supportable
  - Develop plan to migrate tactical architecture and policies to enterprise standards

Contact Information

Contact	Email	Phone
Erik Gerard	Erik.Gerard@impact-advisors.com	440.914.4030
Shefali Mookencherry	Shefali.Mookencherry@impact-advisors.com	847.436.6641

Follow our Impact

Read our Blog

Impact Insights

Questions?

Thank you

Impact advisors