

Defence Outside the Corporate Firewall

What is the “New Normal” and what are the implications for Cybersecurity?

Justin Malczewski

Regional Sales Manager

CrowdStrike

Past-President

Director, Academic Outreach

ISACA Vancouver Chapter

May 27, 2020



Ministry of
Citizens' Services



Guys...Really?

**Are you ladies
doing this?**



OCIO

OCIO
CIRMO

OCIO
DPD

OCIO
ES

SBC

GDX

RPD

ICT

PSD

CSD

Oops....

**How did that get in
here?!**



OCIO

OCIO
CIRMO

OCIO
DPD

OCIO
ES

SBC

GDX

RPD

ICT

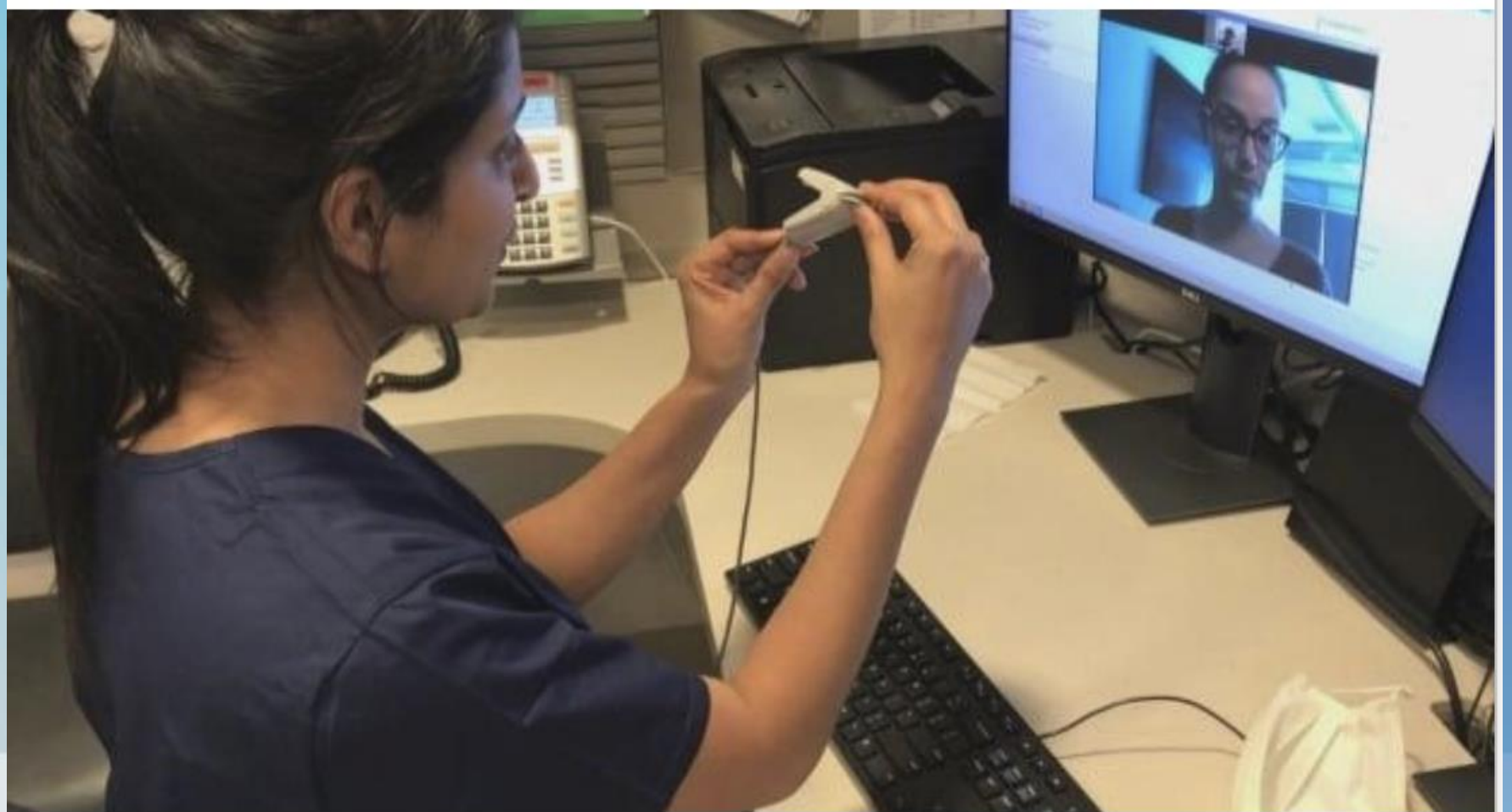
PSD

CSD



Remote Working: Is this the new normal?

Telemedicine



After the pandemic, some patients and doctors hope virtual house calls are here to stay | CBC News

[cbc.ca](https://www.cbc.ca) • 4 min read

Even after the crisis eases, companies may let workers stay home. That would affect an entire ecosystem, from transit to restaurants to shops. Not to mention the tax base.

Real Estate

NEW YORK The New York Times SUBSCRIBE NOW LOG IN


The Coronavirus Outbreak | **LIVE** Latest Updates Maps and Tracker States Reopening Living at Home Newsletter

ADVERTISEMENT

Ad closed by Google

Manhattan Faces a Reckoning if Working From Home Becomes the Norm

Even after the crisis eases, companies may let workers stay home. That would affect an entire ecosystem, from transit to restaurants to shops. Not to mention the tax base.



Companies of all sizes are evaluating their need for office space during the coronavirus pandemic, with potentially profound implications for New York City. Chang W. Lee/The New York Times

By **Matthew Haag**

Published May 12, 2020
Updated May 13, 2020

f t v s b

Government holds first-ever virtual House of Commons session

The government is using popular video conferencing platform Zoom



By Aisha Malik @AiishaMalik1 APR 28, 2020 | 1:50 PM EDT | 0 COMMENTS



Government

**On Behalf of Students & Parents:
A HUGE SHOUT OUT to our Teachers
and all of the people who support
them in the Province of BC!!**

Many challenges.....

.....but there are opportunities as well!

Education



Ministry of
Citizens' Services

Community update: BCIT continues to monitor COVID-19

Updated: May 22, 2020 – 10:25 am

An update from President Kathy Kinloch



THE UNIVERSITY OF BRITISH COLUMBIA

Coronavirus (COVID-19) and UBC's response

[Home](#) [Prevention](#) [Student FAQs](#) [Faculty & Staff FAQs](#) [Resources](#)

Coronavirus (COVID-19) and UBC's response



Coronavirus COVID-19

BC Centre for Disease Control | BC Ministry of Health



HOW YOU CAN SLOW THE SPREAD OF COVID-19

Take care of others by
taking care of yourself.

Wash your hands, don't touch
your face, and stay home if
you are sick.

Stay at Home and
Physically Distance

Stay at home whenever you can.
Maintain 2 meters distance from
those outside of your household.

COVID-19 Public Health Guidance for K-12 School Settings

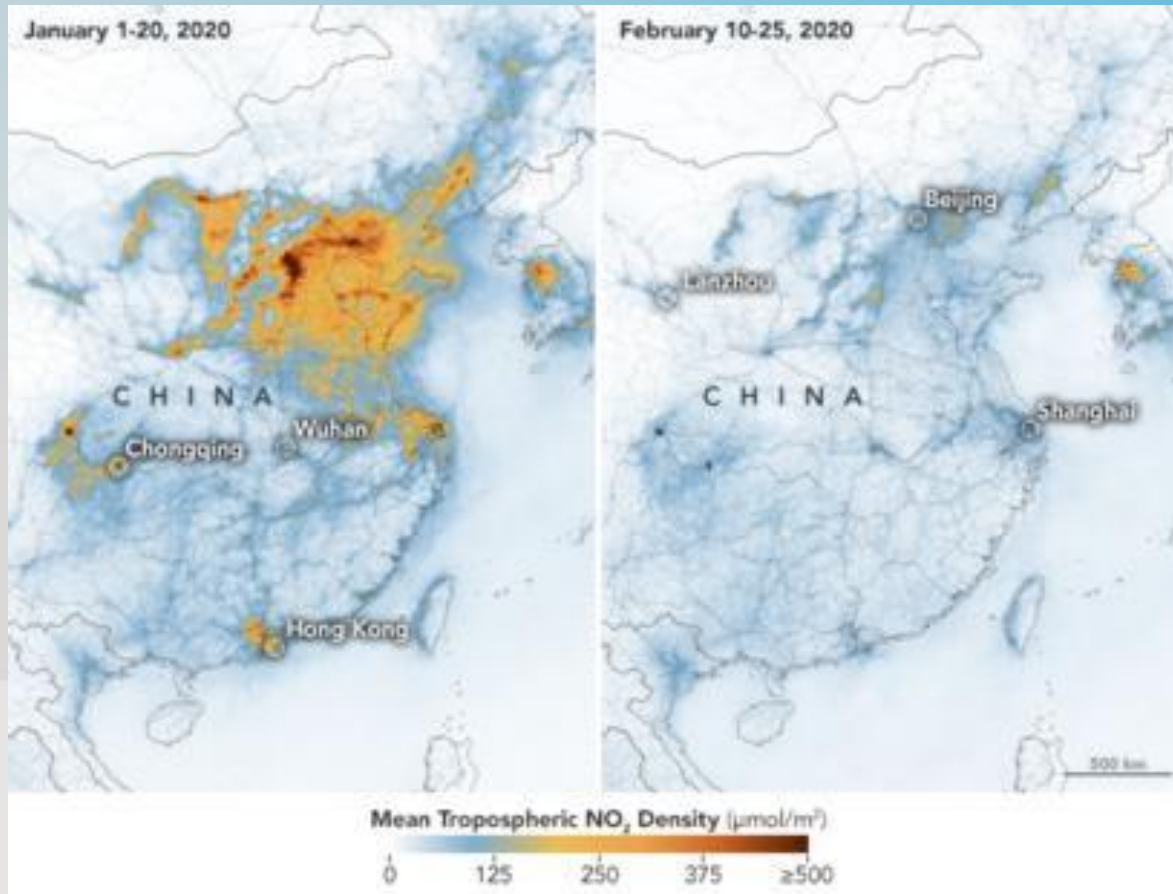
UPDATED: May 19, 2020

**Will you think twice before you book your next flight?
What about for business? Or leisure? Will our employers even
allow us to travel??**

Air Travel



Climate Change: Is this a silver lining?



It's Earth Day today. Happy Earth Day. Do we think the Earth is happy though? Do you think Mother Earth is trying to tell us something? Perhaps a respiratory based virus causing a global pandemic which reduces the air pollution humans create by 25% - 60% in major cities is something we need to take to heart? It is after all, the only Earth we have. Hmmmmm...
#earthday2020 #oneearth #pattysimple #changeisacoming



CNN.COM

Air pollution falls by unprecedented levels in major global cities during coronavirus lockdowns

Connection & Community



Forbes: May 14, 2020

The Coronavirus Just Ripped Open Every Company's Virtual Defenses

Every Company's "Attack Surface" Just Exploded

<https://www.forbes.com/sites/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/#3094a465577c>

EDITORS' PICK | 39,339 views | May 18, 2020, 04:29pm EDT

Hackers Claim Trump Dirty Laundry Data Has Been Sold To 'Interested Party'



Davey Winder Senior Contributor

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

Forbes

Forbes

Business

Small Business

Lifestyle

Lists

184,346 views | May 14, 2020, 09:00am EDT

Why The Largest Cyberattack In History Will Happen Within Six Months



Stephen McBride Contributor

Markets

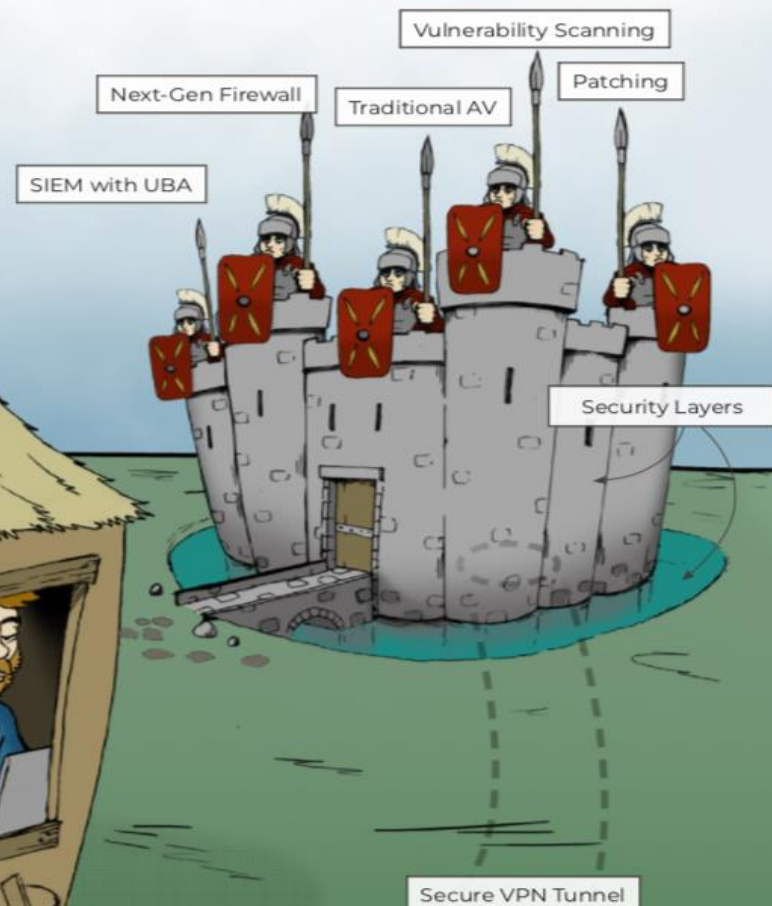
The editor of RiskHedge Report



NATION STATE +
E-CRIME ADVERSARIES

REMOTE
WORKERS

TRADITIONAL
ENTERPRISE



Poll Question

Have you observed an increase in the number of phishing and vishing attempts since COVID-19 social distancing and work-from-home policies were implemented in mid-March?

- 1. No Change**
- 2. I haven't noticed**
- 3. I have seen an increased number of attempts**
- 4. OMG, this is getting ridiculous...the number of phishing emails and/or vishing phone calls I'm getting is off the charts!**

Current Threat Profile

Interestingly, the number of Phishing Emails hasn't necessarily increased....

But

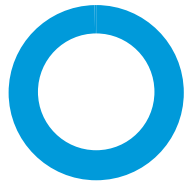
- The shift to COVID related techniques is almost absolute
- We've never seen threat actors en masse exploit a single theme like this

What's New

- Distracted, stressed employee base
- WFH workforce
- IT Help Desks far away
- Sophistication

Attacks increasingly target people, not infrastructure

THREATS USE SOCIAL ENGINEERING, NOT VULNERABILITIES



95%+

Malware attacks rely on user to run malicious code



300%+

Increase in corporate credential phishing

Source: Proofpoint Threat Data.

SHIFT TO CLOUD CREATES NEW THREAT VECTORS, DATA EXPOSURE



Account takeover of cloud apps is a growing problem

71%

Orgs exposed to targeted attacks

37%

Orgs detected successful breach

Source: Proofpoint Threat Data.

EMAIL FRAUD IS A BOARD-LEVEL ISSUE



\$27B+

Direct losses worldwide (Oct 2013–May 2018)

170K+

Incidents worldwide since June 2016

Source: FBI.

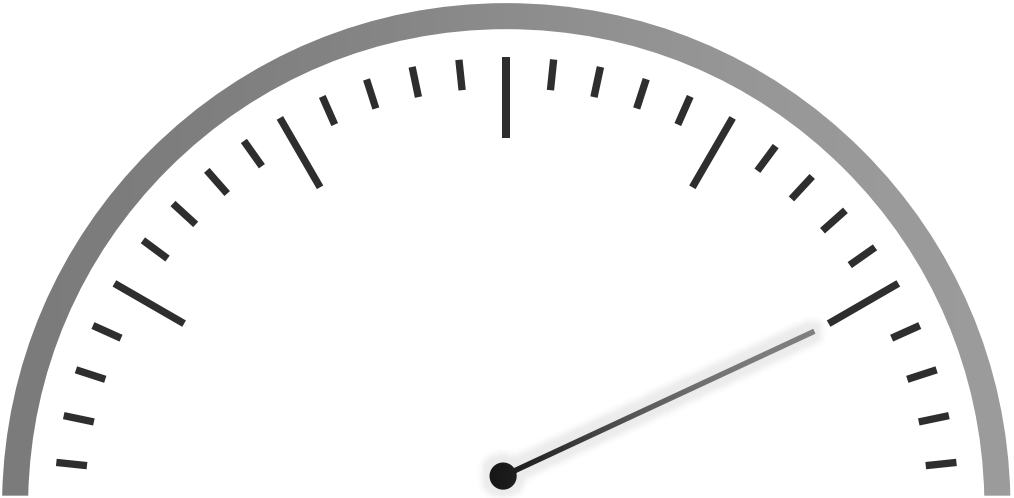
COVID-19 Volume April 2020

Unique Campaigns Tracked

Message context

| | |
|-------------|----------|
| Messages | 400,000+ |
| URLs | 300,000+ |
| Attachments | 200,000+ |

375+



Lures

Novel Coronavirus (COVID-19) Update - Temporary Items

Coronavirus (2019 -nCoV) Safety Measures - Temporary Items

Message

Coronavirus (2019 -nCoV) Safety Measures

DL Dr Liang-Hai Sie <liang-hai@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety... 1.6 MB

Download All Preview All

Dear Sir/Madam,

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

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficult


Regards

Dr Liang-Hai Sie

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

 World Health Organization

Important: COVID-19 Update on corona virus for your safety. - Temporary Items

Message

Important: COVID-19 Update on corona virus for your safety.


CH CDC Health Care

Sunday, March 15, 2020 at 1:00 AM

Show Details

Information_corona... 14.3 KB

Download All Preview All



Dear [redacted]


In order to ensure you have relevant information as we deal with the COVID 19 virus,

we have put together an information sheet in the attached that we hope is helpful and answers some questions you may have.

Let's fight against Corona Virus (COVID-19)

Thank you

Centers For Disease Control and Prevention
saving Lives protecting people.



Coronavirus advisory information - Alert!! and Health Warning. [EXTERNAL]

World Health Organization (WHO) <noreply-whohelpdesk-yttre-7yewas-576999-cb06-o...

g as a

rtness of breath and
severe acute

The World Health Organization Team



Increase in Active Adversaries on Networks

83% eCrime, 17% Nation-State

eCrime Top 5 Industries:

- Technology
- Financial
- Manufacturing
- **Healthcare**

Nation-State Top 5 Industries:

- Telecommunications
- Manufacturing
- **Healthcare**
- Media
- **Government**

Nation-State Active Adversaries:

Panda (China)
Kitten (Iran)
Chollima (North Korea)

Jennifer Ayers, VP OverWatch

Falcon OverWatch has observed a 50% increase in distinct and sophisticated intrusions since Jan 2020 from the previous quarter. A strong contribution to this increase is the shift in techniques surrounding Ransomware as a Service by eCrime Adversaries observed in 2019. This change marked a shift in availability of the “affiliate” model allowing for more opportunistic players to take advantage of this space.

Falcon OverWatch Team



Key Factors for Securing a Remote Workforce

Continued education is crucial, particularly as coronavirus-themed scams escalate

(But we can not rely on this alone!)

Make sure you have a current cybersecurity policy that includes remote working

Plan for BYOD (bring your own device) devices connecting to your organization

Be aware sensitive data may be accessed through unsafe Wi-Fi networks

Cybersecurity hygiene and visibility are critical

Crisis management and incident response plans need to be executable by a remote workforce

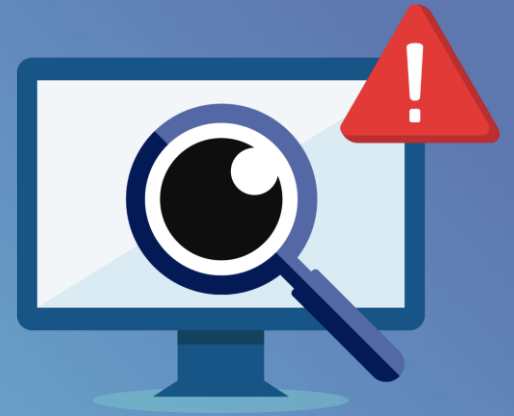
What we need to do is turn the villagers hut into the castle

But, we can't afford to build layered defences in the traditional model and we need to be able to control/operate these defences centrally



Everything starts with....

VISIBILITY!!



And the only place where we can realistically get that visibility is at the gateway (email) and the endpoint....particularly as the perimeter of the network erodes (e.g. Mobility, Cloud) and the network itself is encrypted.

Only with visibility is it possible to make intelligent security decisions (prevention/detection/containment/response)

Next Gen Controls

- Use ***strong passwords*** and implement multi-factor authentication - for everything
- If you use a remote desktop client, ensure it is secure
- Do not forget mobile devices – extend security to all iOS and Android devices
- Teach remote workers how to secure home WIFI networks
- Ensure backup and recovery processes extend to home devices
- Please remember remote collaboration tools to connect with your colleagues, i.e. consider using Zoom for internal face to face meetings

- Patching, Patching, Patching

(CrowdStrike Ecosystem Partner Automox's Mission Statement: Patch Your Sh*t!)

- Implement Best-In-Class Email Protection
- Integrate with Best-in-Class Endpoint Protection for Automated Response
- Visibility & Control Prevention Detection & Response

- Host Based Firewall (prevent lateral movement across home networks)
- Unrealistic to expect all home-based workers to establish these controls

**Centralized
Management**

Call to Action

Encourage your children, friends, family and/or retrain yourself to enter the exciting field of Cybersecurity!

Some of the most exciting and rewarding jobs of the future!

Justin Malczewski
Director Academic Outreach
ISACA Vancouver Chapter

justin.malczewski@crowdstrike.com

604-868-0267



Ministry of
Citizens' Services