Cybersecurity of remote work

28 SEPTEMBER 2020

Tamas Gaidosch

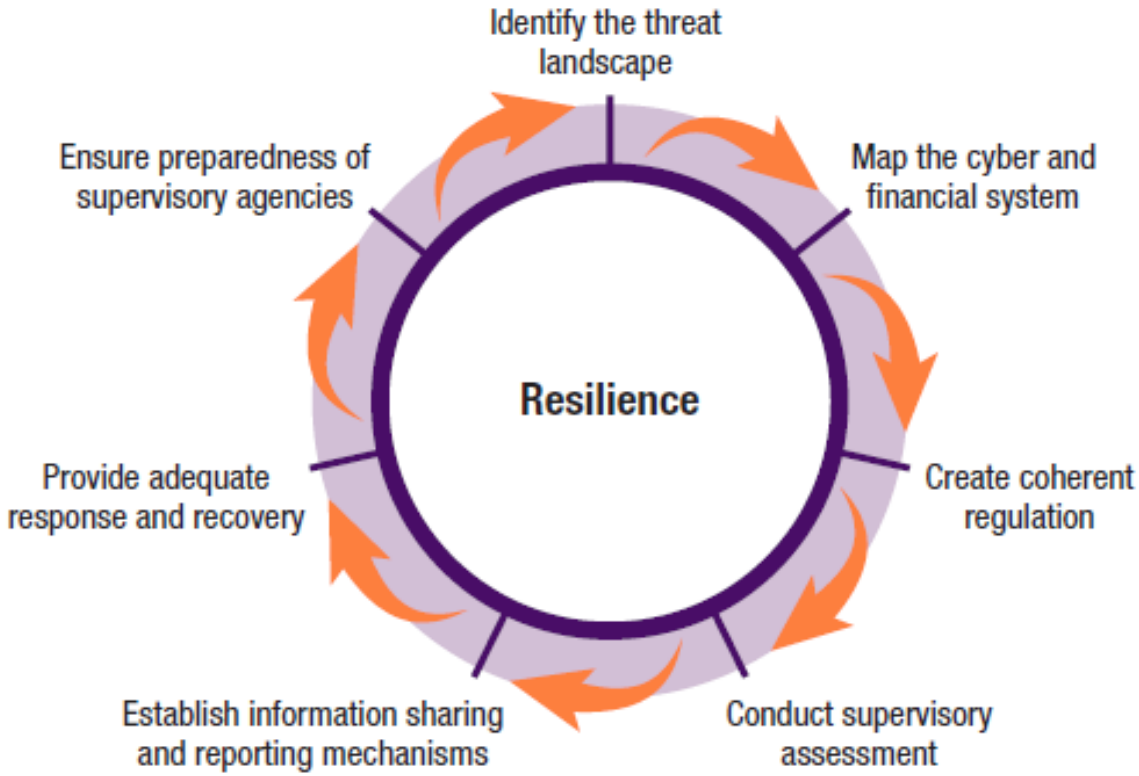
Agenda

How does supervision build cybersecurity resilience?

What are the cybersecurity risks of working remotely?

Recommendations

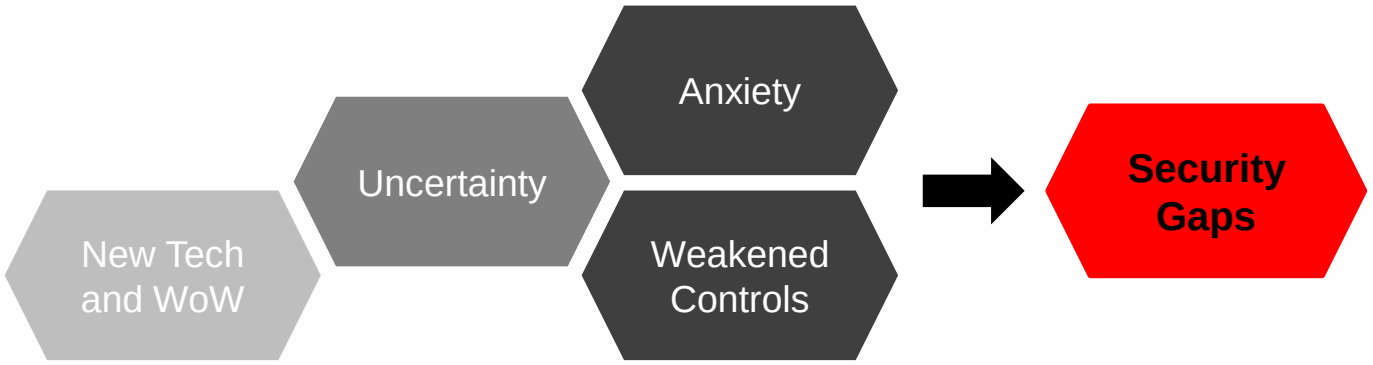
The supervisor´s role



Source: IMF staff.

https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238

The threat landscape now



Nothing fundamentally new, but heightened

- Rapid shift to tele-work
- Unvetted new tools and services (including the cloud)
- Urgency to deploy relief packages

Just how much heightened?

by DH Kass • Apr 19, 2020

Online crimes reported to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) have roughly quadrupled since the coronavirus (Covid-19) pandemic, a senior cybersecurity official said in a webinar hosted by the Aspen Institute last week.

The number of cybersecurity complaints to the IC3 in the last four months has spiked from 1,000 daily before the pandemic to as many as 4,000 incidents in a day, said Tonya Ugoretz, the deputy assistant director of the FBI's cyber wing, *The Hill* reported.

autoblog RESEARCH BUY NEWS & REVIEWS OWNERSHIP VIDEOS Make

OFFICIAL

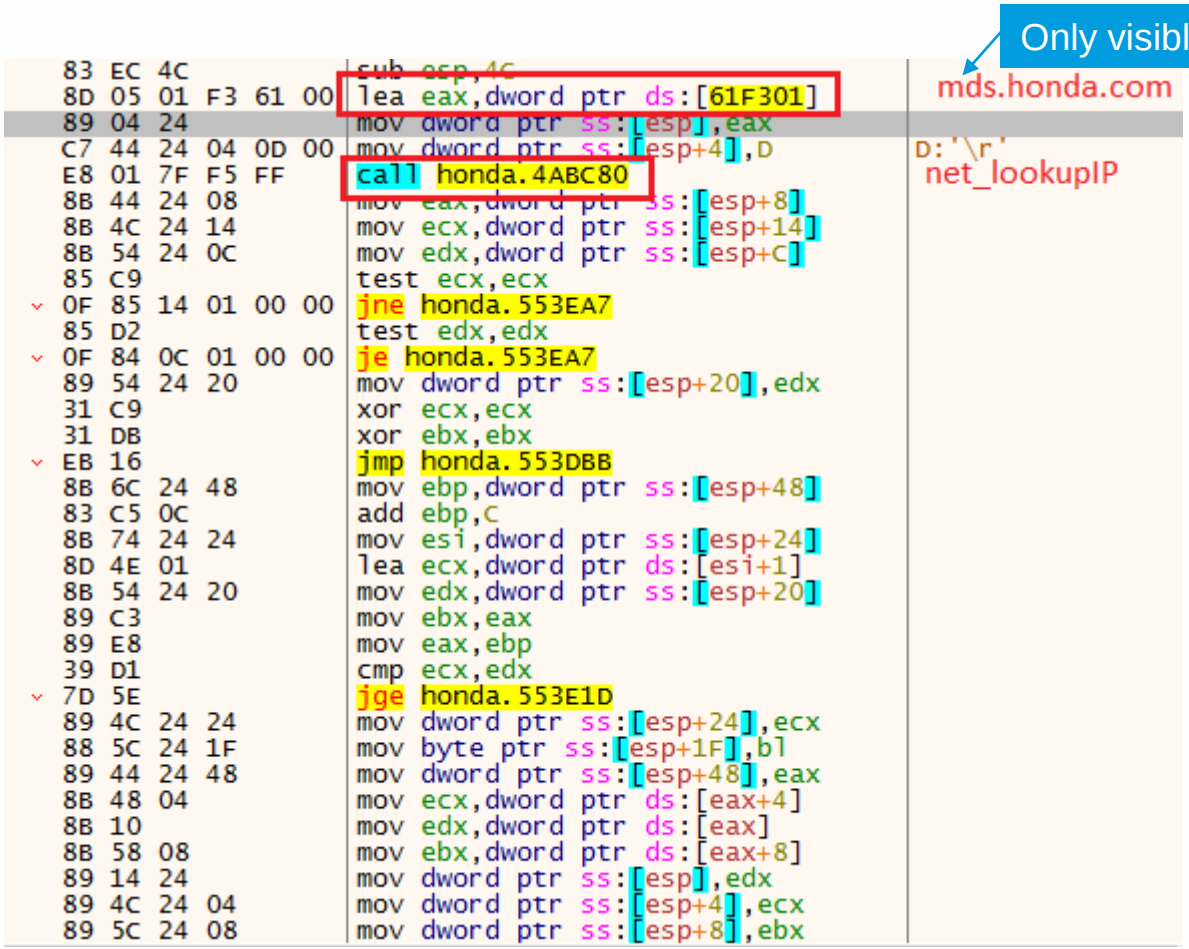
Honda production knocked offline by ransomware cyberattack

Work at several plants, including main factory in Ohio, has been suspended

JEREMY KORZENIEWSKI

Jun 9th 2020 at 9:17AM

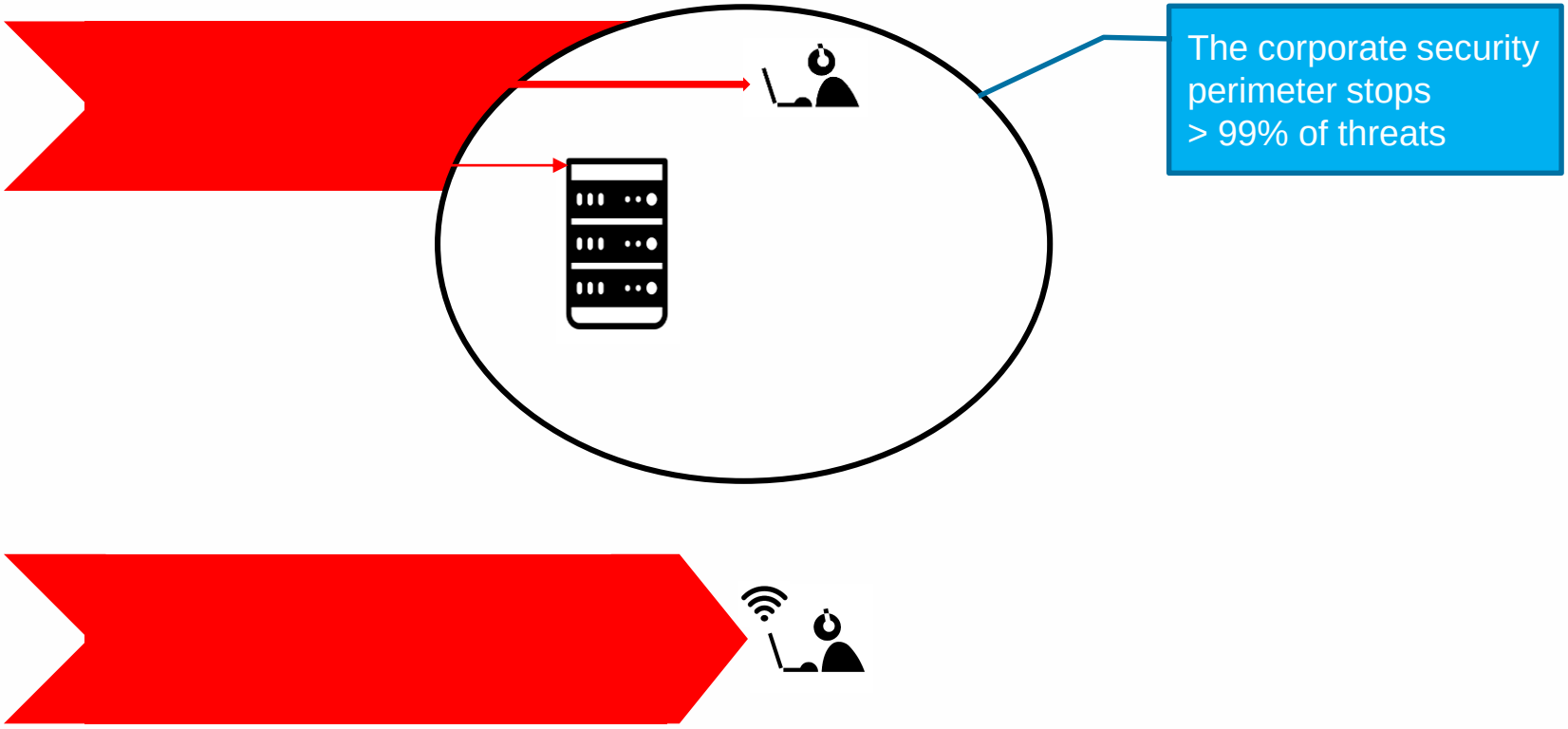
A highly targeted attack



Payload launch decision sequence, reverse engineered

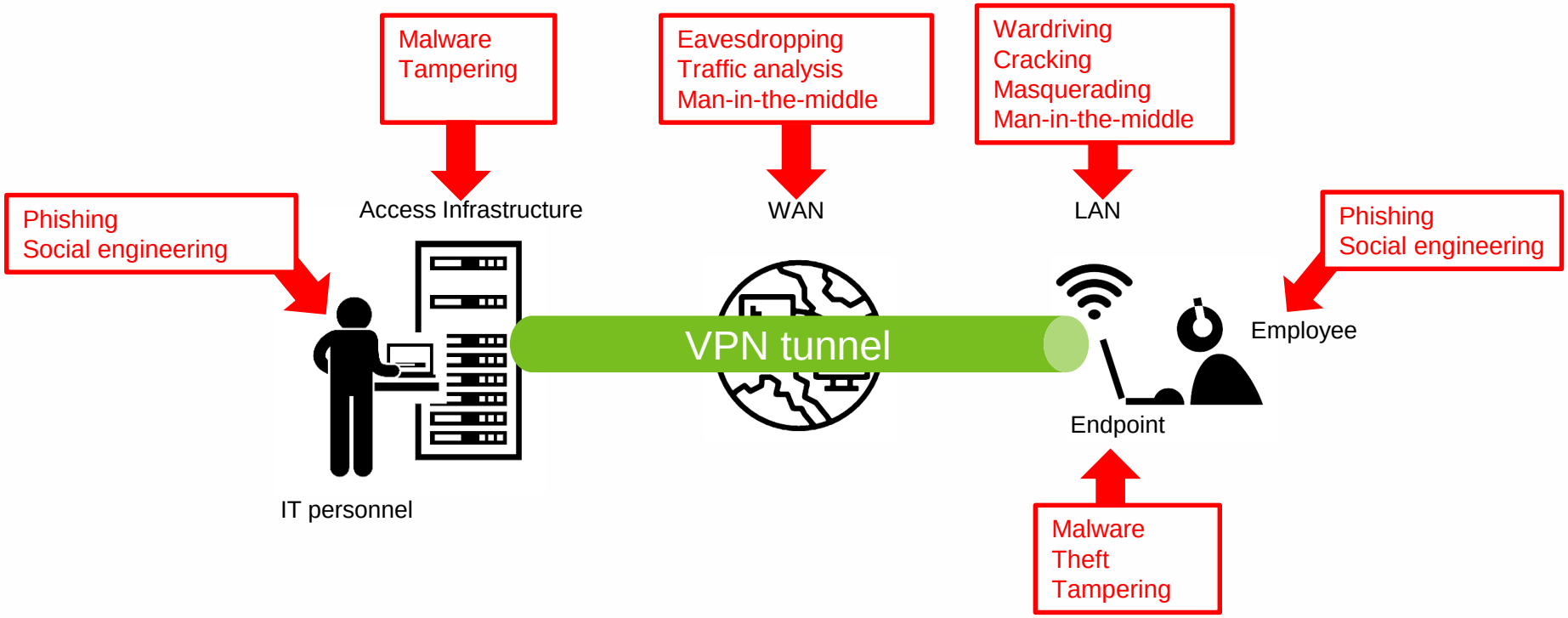
Source: Malwarebytes Labs

Why are attackers so active?



Unprecedented exposure

Threat landscape of remote work



Risk: weak infrastructure

Not designed for large-scale and prolonged usage

Inadequate capacities

- Low number of concurrent users
- Low number of notebooks and mobile devices
- Limited bandwidth
- Insufficient support

Pressure on IT Departments to find solutions fast

Risk: cloud

Business: Not enough conferencing capacity. Do something. Fast!

IT: We cannot bring in more servers fast… Maybe the cloud?

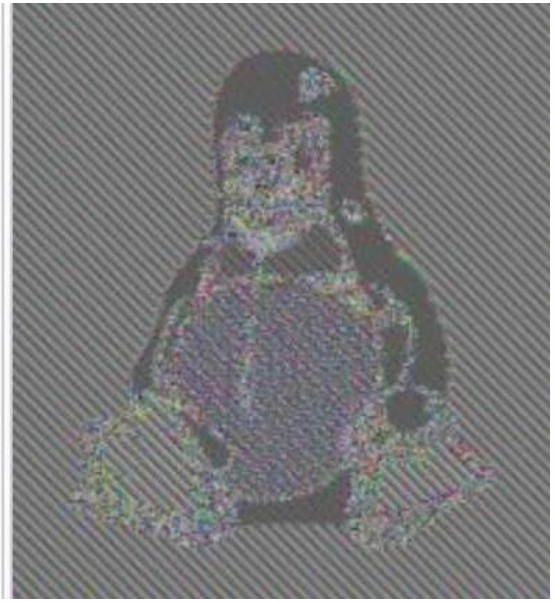
Business: We need it yesterday!

IT: Alright… let's Zoom then!

Poor security design

Bad choice of cryptographic algorithm (AES-128 in ECB mode)

Unencrypted

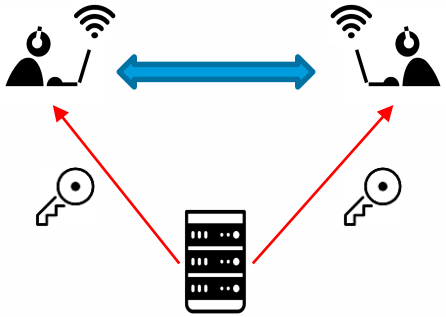


Encrypted the Zoom way

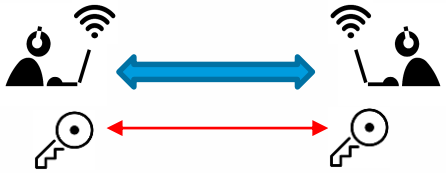
Poor security design

Encryption keys were centrally generated and distributed to participants

Servers could have been compromised and keys stolen



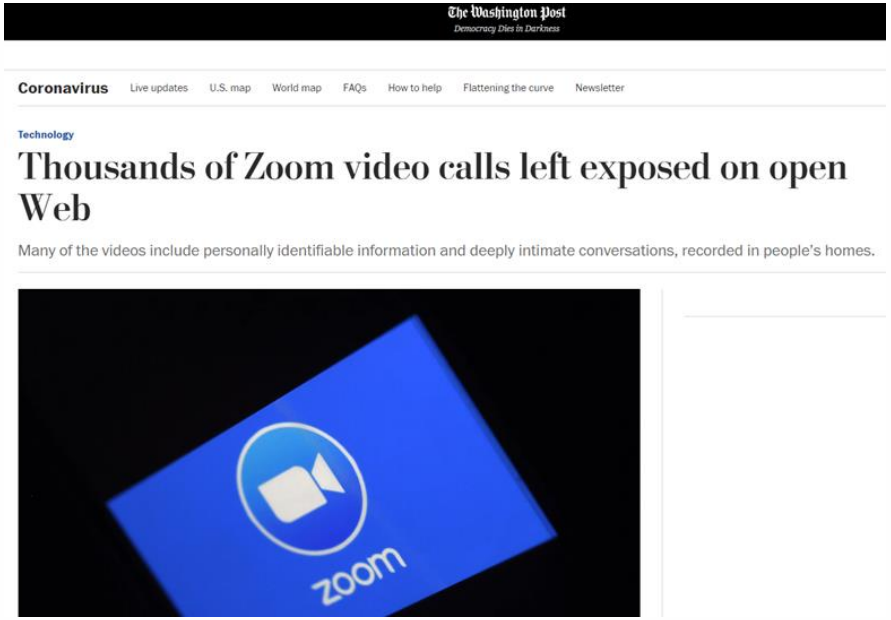
Centralized key generation

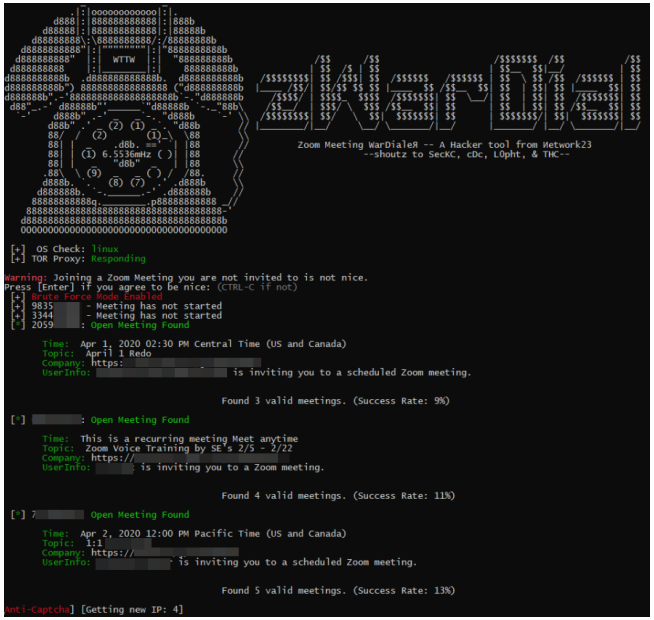


Distributed key generation

Poor security design

Predictable identifiers and insecure cloud configurations have enabled hackers to steal recordings of past meetings and eavesdrop on live meetings

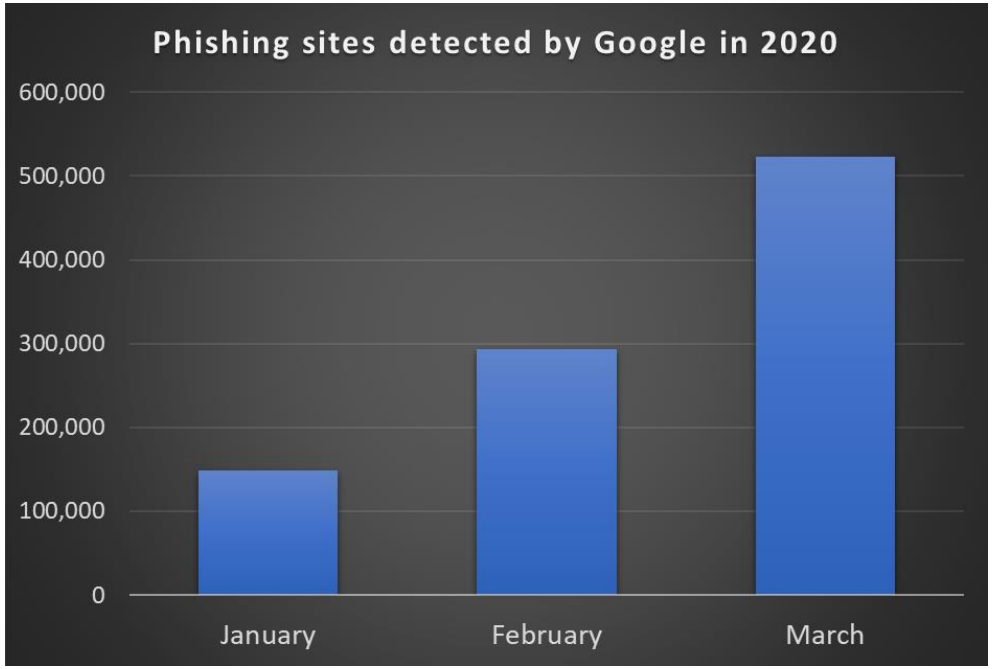




Risk: phishing

~ 90% of successful data breaches start with a phishing attack

~ 23% of targeted people open phishing emails and ~11% click before they think



Source: Google, IMF staff illustration

Example

WH

World Health Organization ‹ [redacted]

[redacted]

Monday, March 23, 2020 at 7:23 PM

Show Details

COVID18-COMPEN...
9.1 KB

Download All Preview All

International Monetary Fund Compensation Unit, London.

In Affiliation With World Bank.

[redacted]

[redacted]

Ref: IMF/UK/0083

Attention Beneficiary

[redacted],

How are you today? Hope all is well with you and the family? You may not understand why this mail came to you. We have been having a meeting for the past 3 months which ended yesterday with the Director and secretary to the International Monetary Fund, UN (United Nations) and WHO (World Health Organization). You have been selected randomly to be compensated financially due to the outbreak of the COVID-19 Epidemic outbreak.

You will be paid through our paying center in london for your compensation payment from the International Monetary Fund Office treasury account.

Find attached "COVID-19-Compensation" receipt, view attached file to print your winning confirmation.

Thanks and God bless you and your family, don't neglect this I advice you.

International Monetary Funds, Making the world a better place.

Recommendations

Authorities and firms should prioritize

- Clear remote access policies (who, what, when, and how)
- Robust authentication of users and devices
- Strong encryption methods
- Secure remote access devices (endpoint security)
- Network security monitoring

Cloud usage should be based on detailed risk assessments

Additional user awareness campaigns should be launched

Robust controls over configurations at both ends of the connection

Additional security controls for critical functions

How should regulation adapt?

Now is not the time for major changes in cybersecurity regulation

Definitely do not relax requirements

Consider specific guidance (e.g. based on the Cybersecurity of Remote Work note)

- Stay principles-based but offer examples of good practice
- Link to the more general IT or operational risk management requirements

What should supervisors do?

Strengthen off-site supervision

- Contingent on resources and data availability

Redesign on-site supervision

- As “contactless” as possible
- Temporarily less intrusive
- More risk focused (e.g. on remote access)
- Reduce the scope and relax the schedule if needed
- Little need to relax requirements on evidence strength
- Offset the lower assurance with additional procedures when back to normal

Cyber hygiene – it is not too difficult!

Pay attention to physical security

Protect your WiFi

Keep work and home separate

Apply updates regularly

Do no open suspicious content

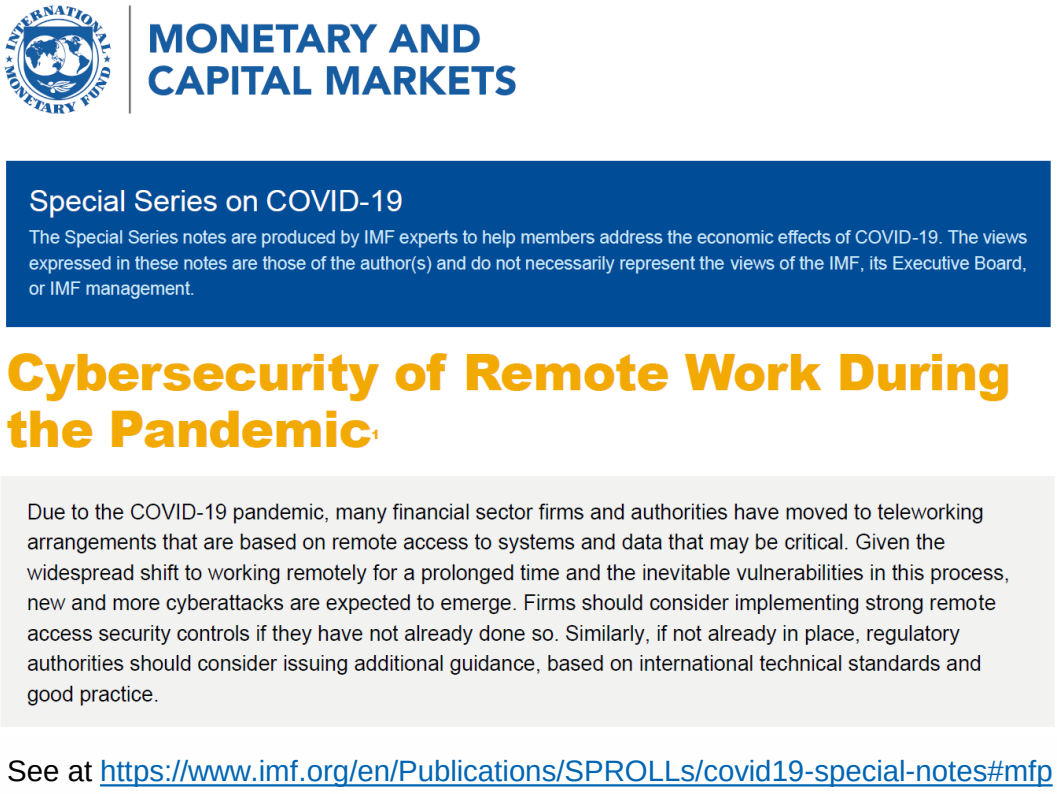
Cover your webcam when not in use

Work under regular user accounts

Use strong passwords / 2FA

Protect videoconferences

For further details



MONETARY AND CAPITAL MARKETS

Special Series on COVID-19

The Special Series notes are produced by IMF experts to help members address the economic effects of COVID-19. The views expressed in these notes are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Cybersecurity of Remote Work During the Pandemic

Due to the COVID-19 pandemic, many financial sector firms and authorities have moved to teleworking arrangements that are based on remote access to systems and data that may be critical. Given the widespread shift to working remotely for a prolonged time and the inevitable vulnerabilities in this process, new and more cyberattacks are expected to emerge. Firms should consider implementing strong remote access security controls if they have not already done so. Similarly, if not already in place, regulatory authorities should consider issuing additional guidance, based on international technical standards and good practice.

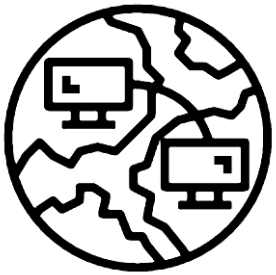
See at https://www.imf.org/en/Publications/SPROLLs/covid19-special-notes#mfp

One last thing…

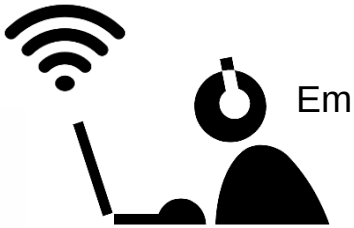
Access Infrastructure

IT personnel

WAN



LAN



Employee

Endpoint

THINK END-TO-END

Thank you!