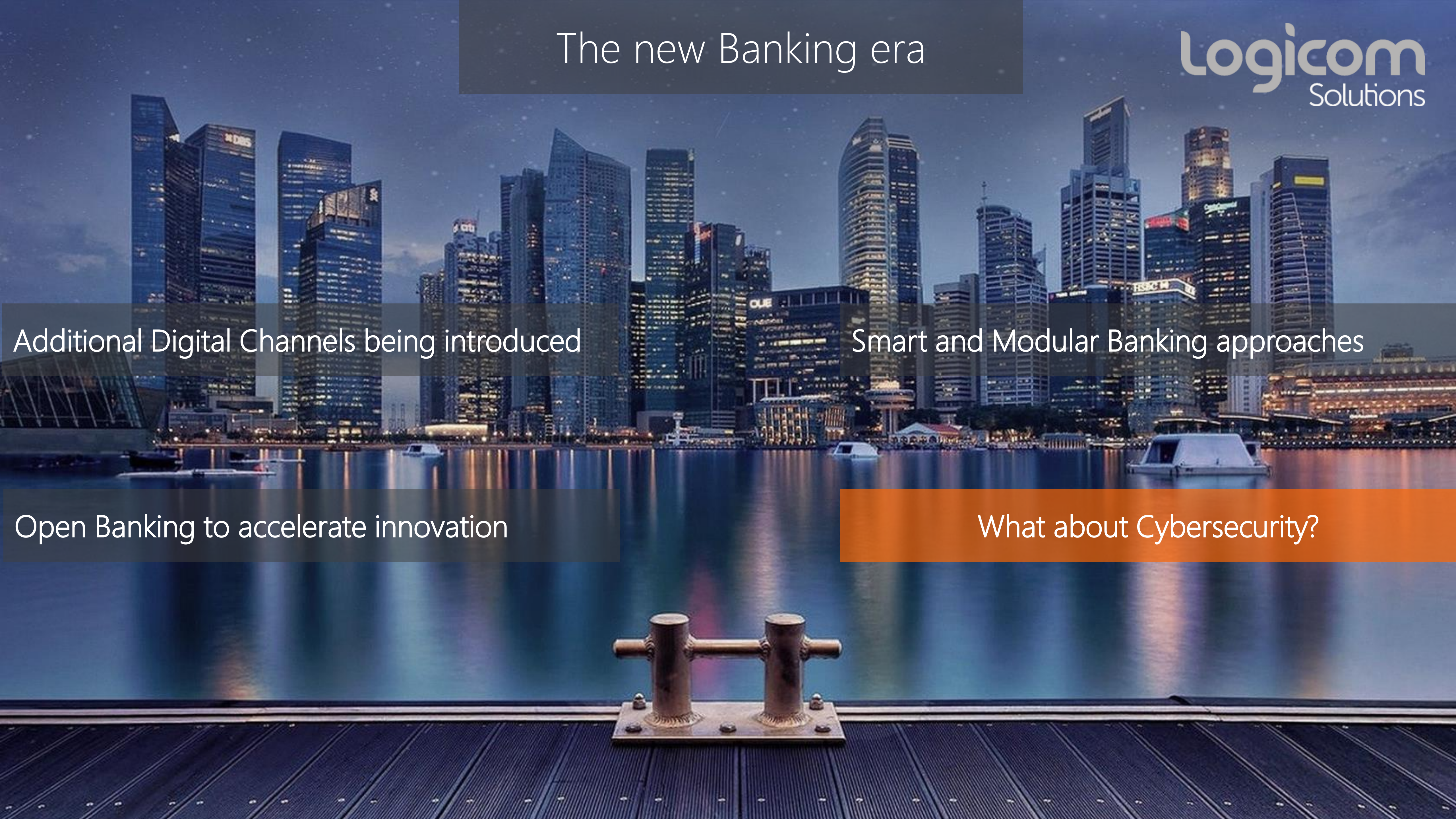
logicom Solutions

Cybersecurity incidents on the rise

A FALSE SENSE OF SECURITY

BUSINESS CONSULTING SERVICES

The new Banking era



Additional Digital Channels being introduced

Smart and Modular Banking approaches

Open Banking to accelerate innovation

What about Cybersecurity?

Logicom Solutions

1 **Attacks targeting less secure elements**
Supply Chain Attacks

2 **Fraudulent activities from global pandemic**
Advanced Phishing Techniques

3 **Exposure from unpredicted scenarios**
Breach of physical security

> “ It is a **world-class** and **industry leading** vendor! We can **blindly** trust them!

A FALSE SENSE OF SECURITY

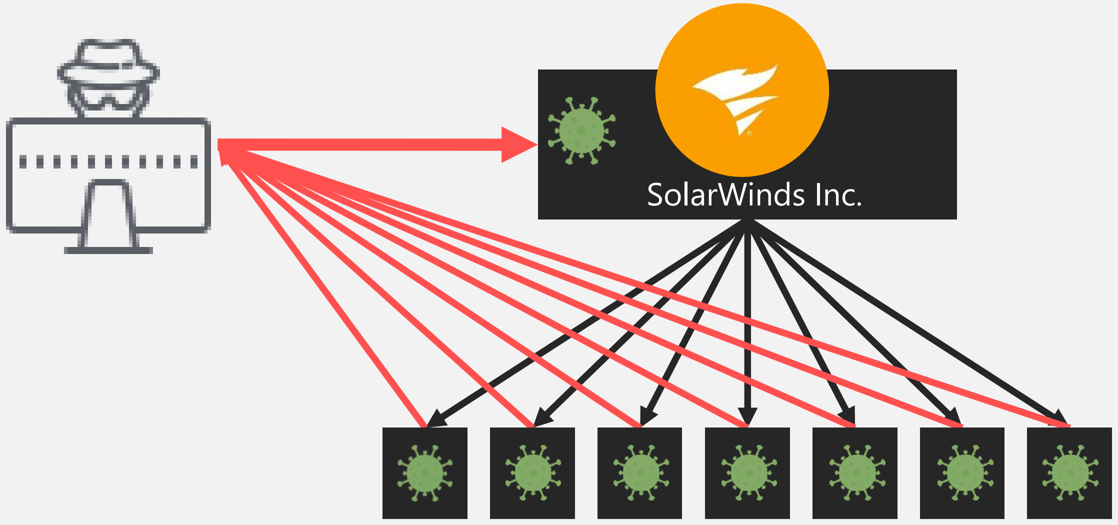
- SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure.

- It had about 300,000 customers as of December 2020, including nearly all Fortune 500 companies and numerous federal agencies.

SolarWinds Inc.

THE SOLARWINDS HACK

HOW IT HAPPENED



18.000

customers have been affected

INCIDENT TIMELINE

MAR 2020

4 5 6 7 8 9 10 11

DEC 2020

CYBERSECURITY INCIDENT HAPPENED

CYBERSECURITY INCIDENT WAS UNCOVERED

Logicom Solutions

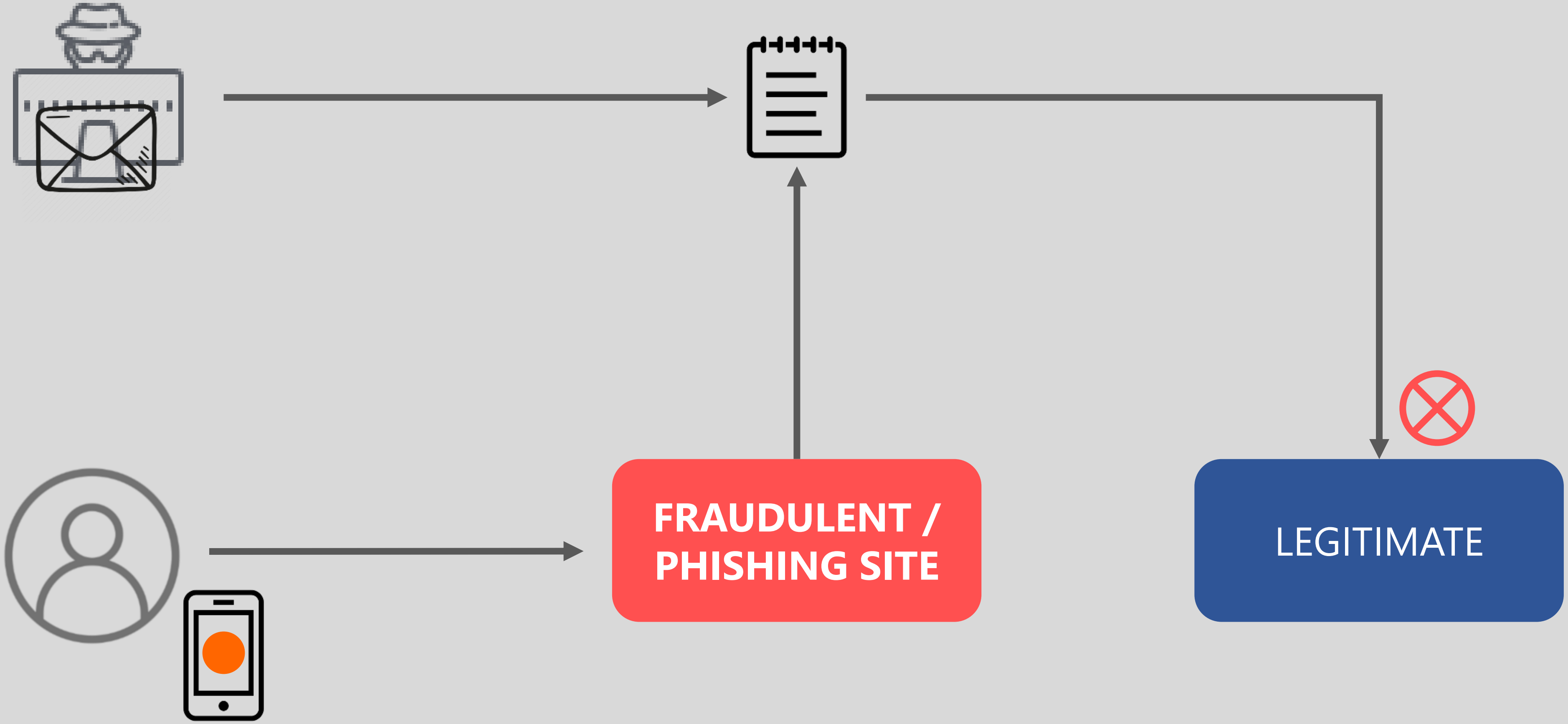
> “ We have safeguarded our WFH users from phishing attacks, by enforcing MFA.

A FALSE SENSE OF SECURITY

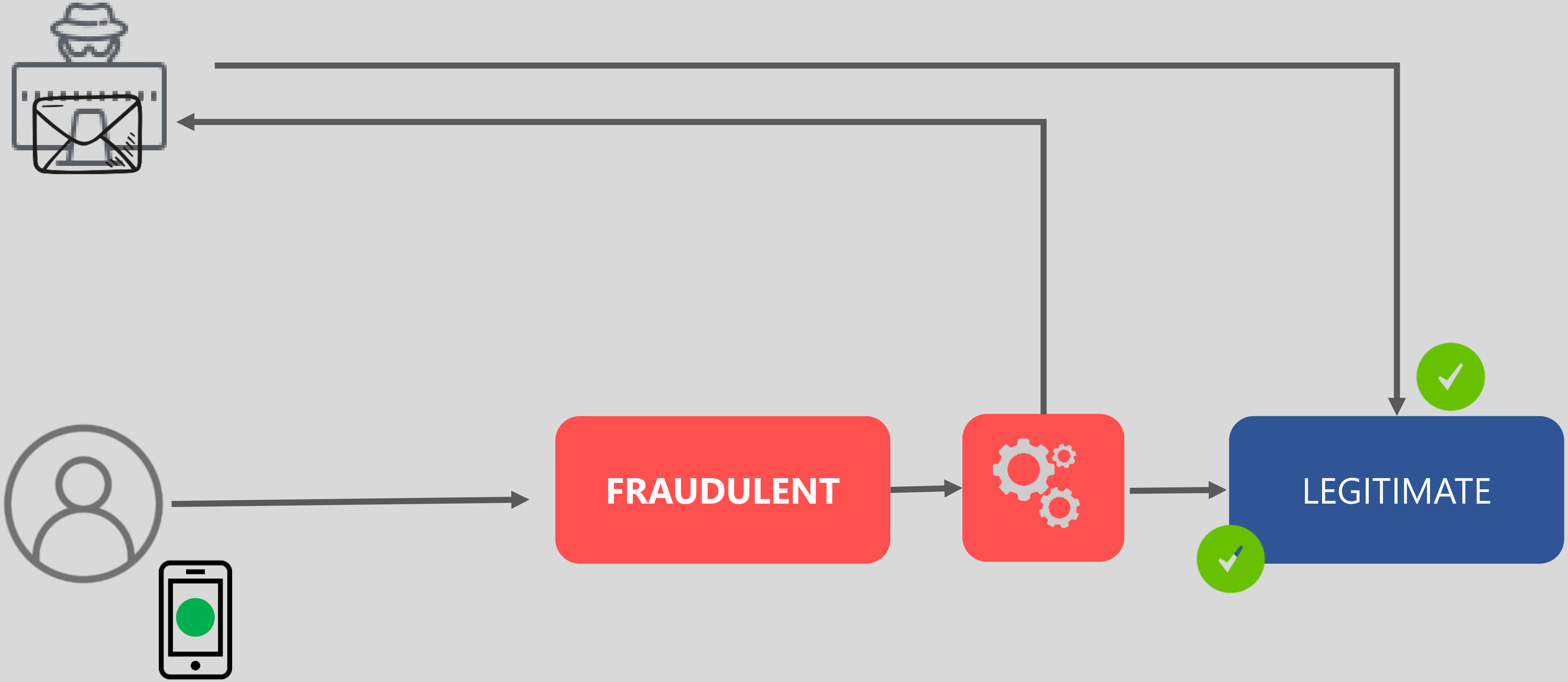
Logicom Solutions

A rise in advanced **phishing** attacks

A TRADITIONAL PHISHING ATTACK



ADVANCED PHISHING ATTACK



Logicom Solutions

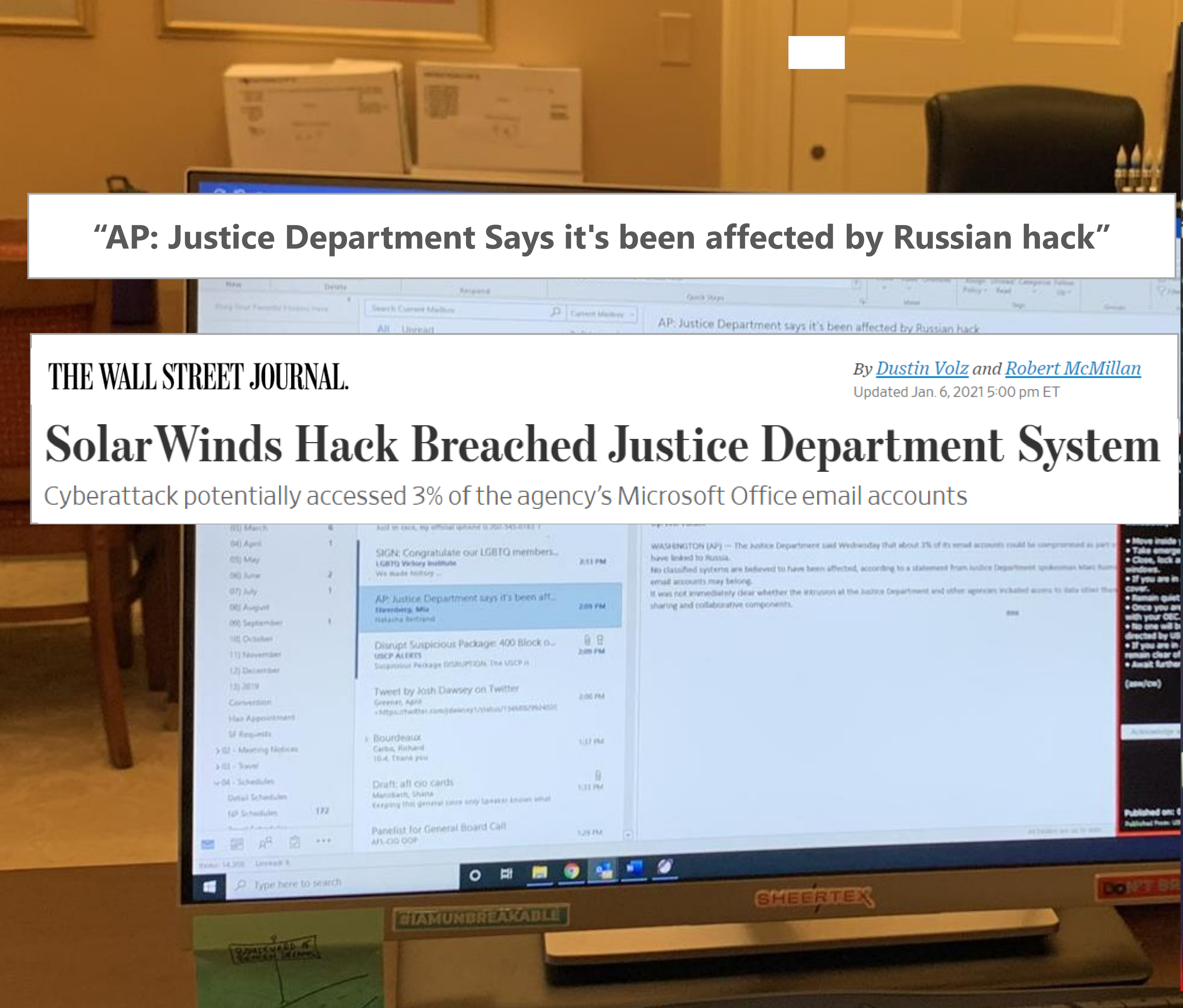
> “Physical security is not a major concern. Who can get into our building?

A FALSE SENSE OF SECURITY

Logicom Solutions

Logicom Solutions

Reuters



“AP: Justice Department Says it's been affected by Russian hack”

THE WALL STREET JOURNAL.

By Dustin Volz and Robert McMillan
Updated Jan. 6, 2021 5:00 pm ET

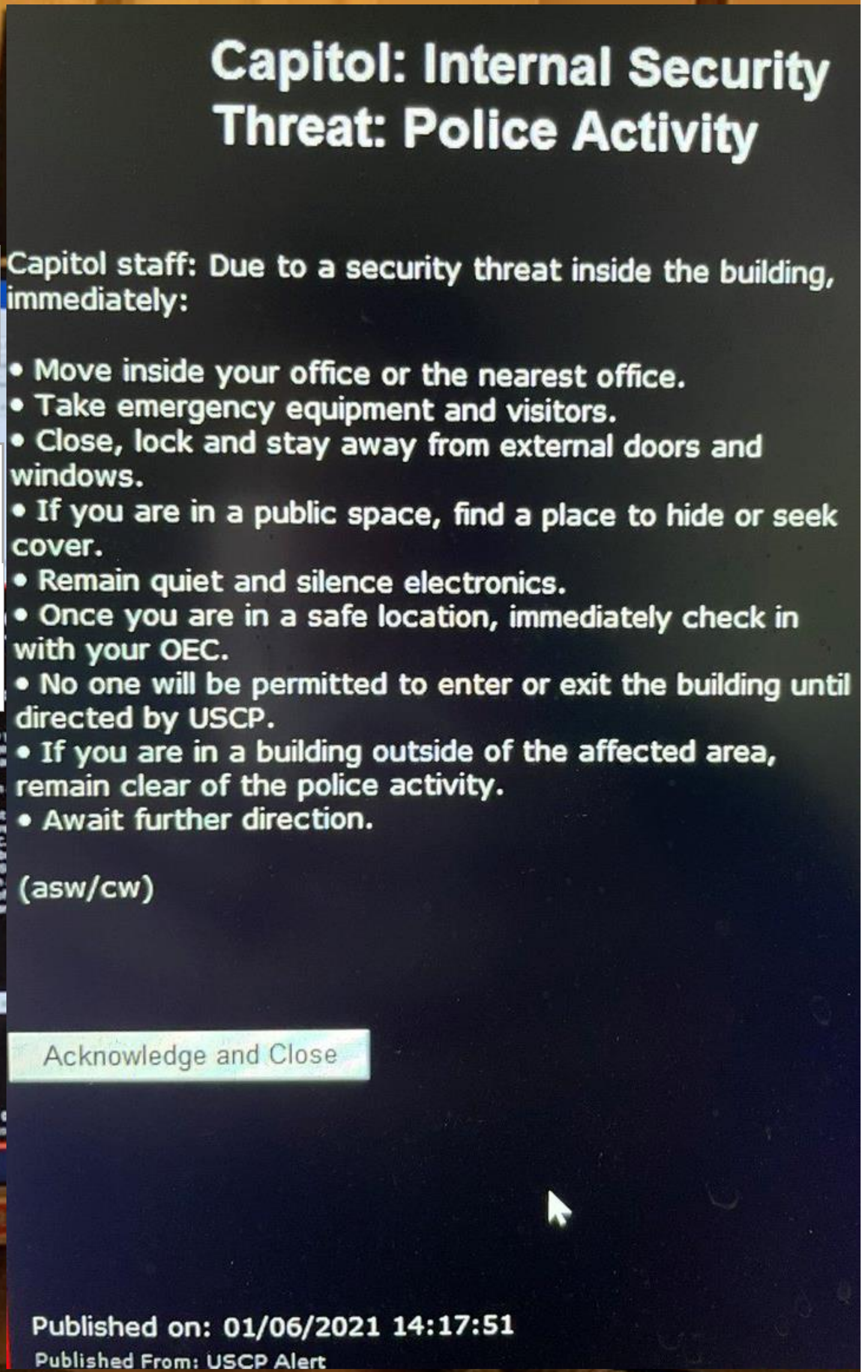
SolarWinds Hack Breached Justice Department System

Cyberattack potentially accessed 3% of the agency’s Microsoft Office email accounts

AP: Justice Department says it's been affected by Russian hack

WASHINGTON (AP) — The Justice Department said Wednesday that about 3% of its email accounts could be compromised as part o
have linked to Russia.
No classified systems are believed to have been affected, according to a statement from Justice Department spokesman Marc Raimo
email accounts may belong.
It was not immediately clear whether the intrusion at the Justice Department and other agencies included access to data other than
sharing and collaborative components.
###

SIGN: Congratulate our LGBTQ members...
AP: Justice Department says it's been aff...
Disrupt Suspicious Package: 400 Block o...
Tweet by Josh Dawsey on Twitter
Bourdeaux
Draft: afl cio cards
Panelist for General Board Call
Type here to search
SHEERTEX
#IAMUNBREAKABLE



Capitol: Internal Security Threat: Police Activity

Capitol staff: Due to a security threat inside the building, immediately:

- Move inside your office or the nearest office.
- Take emergency equipment and visitors.
- Close, lock and stay away from external doors and windows.
- If you are in a public space, find a place to hide or seek cover.
- Remain quiet and silence electronics.
- Once you are in a safe location, immediately check in with your OEC.
- No one will be permitted to enter or exit the building until directed by USCP.
- If you are in a building outside of the affected area, remain clear of the police activity.
- Await further direction.

(asw/cw)

Published on: 01/06/2021 14:17:51
Published From: USCP Alert

logicom Solutions

1

IMPLEMENT ZERO-TRUST MODELS

Strong security controls should be placed, following a zero-trust model and least-privilege principle.

2

INCIDENT RESPONSE READINESS

You cannot improve your readiness when an incident happens. Be well prepared and simulate different scenarios.

3

IN-DEPTH TECHNICAL REVIEWS

General IT Controls are not adequate any more. Technical reviews can provide the insights required for improvement.

4

CONTINUOUS SECURITY AWARENESS

Run a continuous security awareness programme. Human factor is still the weakest link in the security chain.

Logicom Solutions

CHARIS FLORIDES
CISSP, OSCP, MSc in InfoSec

Division Head
Business Consulting Services
Logicom Solutions

Board Member
ISC2 Cyprus Chapter

email address
c.florides@logicom.net

Linkedin Profile
charis.florides