COVID-19, Remote Working and Cyber Attacks

Key considerations for small and mid-size businesses

corix partners

Why?

You are not immune to cyber attacks because you are small

- Data and technology have become central to the business in most companies
- Cyber threats are more active than ever, with firms – large and small – falling victims to indiscriminate cyber attacks on a continuous basis; it is increasingly becoming a matter of **WHEN, not IF**
- Regulation have been tightening world-wide around personal data (GDPR, CCPA and many others), fines are growing and regulators have been targeting all firms irrespective of size (1)

Beyond loss avoidance and business stability, good security and privacy practices build digital trust

- As investors become increasingly ESG-aware, research has started to emerge showing that good security and privacy practices could support higher valuations in some cases as part of the S and G panels of a broader ESG strategy (2)
- As the reflection of good business ethics, they can be turned into a competitive advantage to attract talent, retain customers and become a key ingredient to your mid to long-term “secret sauce”

The COVID-19 crisis does not make those considerations irrelevant

- Social distancing makes people entirely reliant on digital services
- Remote working creates new security imperatives around the way staff collaborate and share information (and around the way cyber security teams need to operate)
- Cyber criminals are targeting the disorganisation created by the crisis and negligent practices (3)
- Good security and privacy practices are key to **KEEPING THE LIGHTS ON**

(1) DLA Piper – GDPR Data Breach Survey (2020) > https://www.dlapiper.com/en/uk/news/2020/01/114-million-in-fines-have-been-imposed-by-european-authorities-under-gdpr/
(2) BCG – Total Societal Impact: A New Lens for Strategy (2017) > https://www.bcg.com/publications/2017/total-societal-impact-new-lens-strategy.aspx
(3) World Economic Forum - Why cybersecurity matters more than ever during the coronavirus pandemic (17 March 2020) > https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

For now, short-term crisis considerations must dominate

Management

Cash flows, supply chains and staff welfare

Right now, cyber attacks and data breaches can only aggravate things

Job preservation and remote working

Staff

Investors

Business stability and resilience

Good Security & Privacy practices are key to **KEEPING THE LIGHTS ON**

But there are probably no silver bullets

Services availability and stability

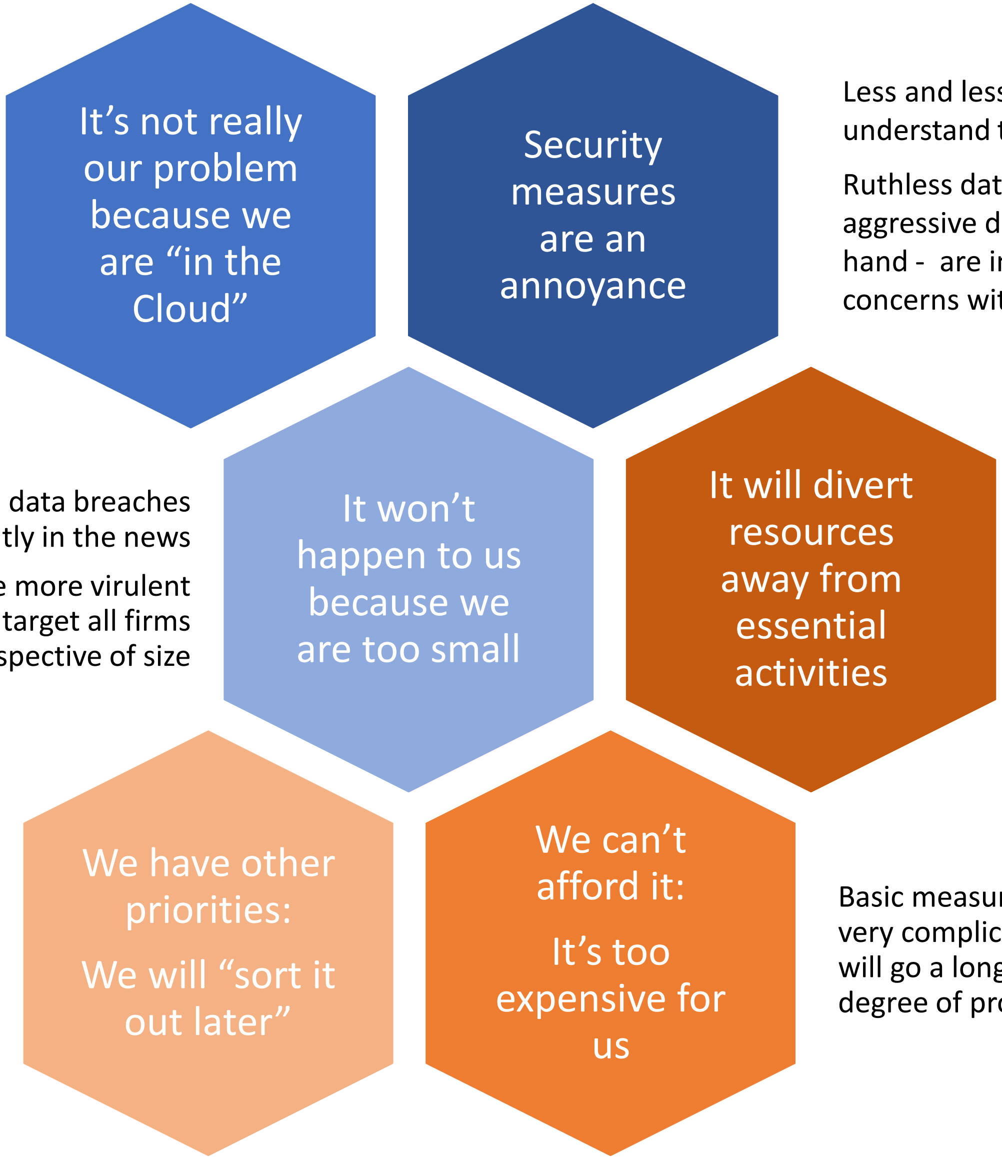
Customers & Markets

Still Some Roadblocks Remain, Preventing Action

- In small and mid-size businesses, the main roadblock is often **a lack of understanding** of what needs to be done now around security to ensure sufficient protection, and how priorities must be set in the current climate in support of the digital, mobile and cloud-based enterprise

- At best, it leads to putting in place isolated and disjointed protective measures

- At worst, senior stakeholders simply **don't know where to start** and some technical illiteracy gives way to mis-conceptions, which – in turn – deprioritise action around security in spite of legitimate and growing concerns



It's not really our problem because we are "in the Cloud"

You remain responsible for the security of your data and liable to your clients in case of breach

The contract with your Cloud provider is likely to be shamelessly one-sided (in their favour)

Security measures are an annoyance

Less and less, as people get hacked and understand the need for stronger security

Ruthless data monetization, personalization or aggressive data surveillance - on the other hand - are increasingly a source of ethical concerns with customers and staff

It won't happen to us because we are too small

Cyber attacks and data breaches are constantly in the news

Cyber threats are more virulent than ever and target all firms irrespective of size

It will divert resources away from essential activities

Security issues will turn customers away in the current climate

Maintaining good security levels is an essential activity and may generate sales if you turn it into a competitive advantage and weave it into your USP

We have other priorities:

We will "sort it out later"

Incidents are expensive to deal with and retrofitting security and privacy measures under duress after something has happened will be painful

We can't afford it:

It's too expensive for us

Basic measures don't have to be very complicated or expensive and will go a long way to provide a degree of protection

For many firms, remote working is nothing new… but three aspects are

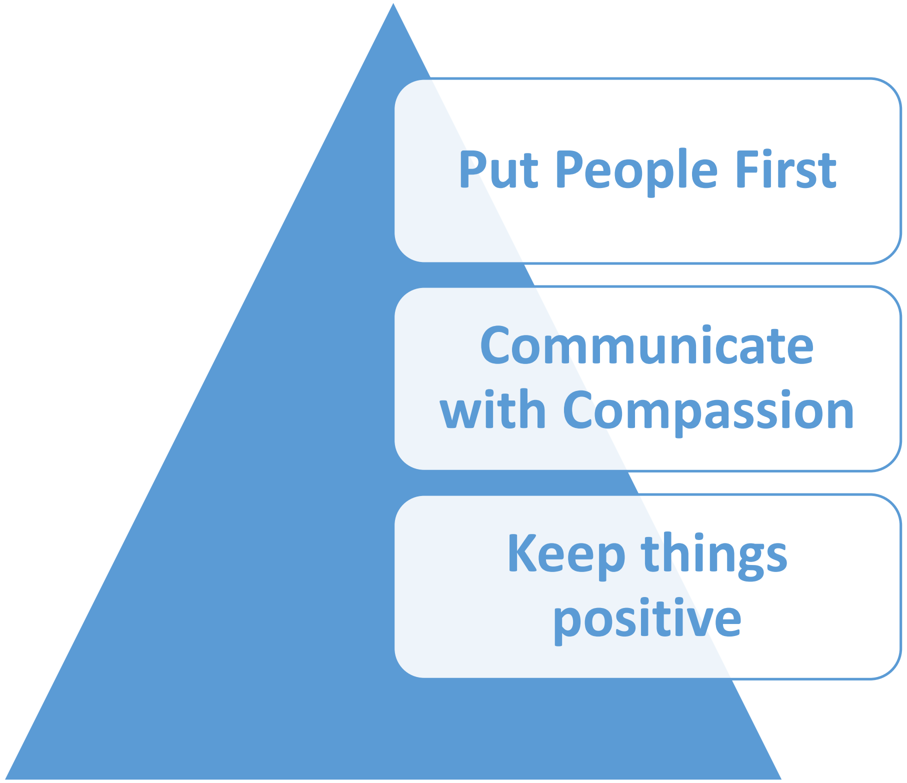
Scale and Speed at which existing remote working solutions have had to evolve

Level of **Stress** (personal and professional) amongst all working communities

Potential **Duration** of the situation and the **Uncertainty** around that

Technology platforms and solutions vary considerably from one firm to another, but **the HUMAN FACTORS are the common denominator**

Large scale remote working presents opportunities for firms to progress on cyber security but they need to act with care



Put People First

Communicate with Compassion

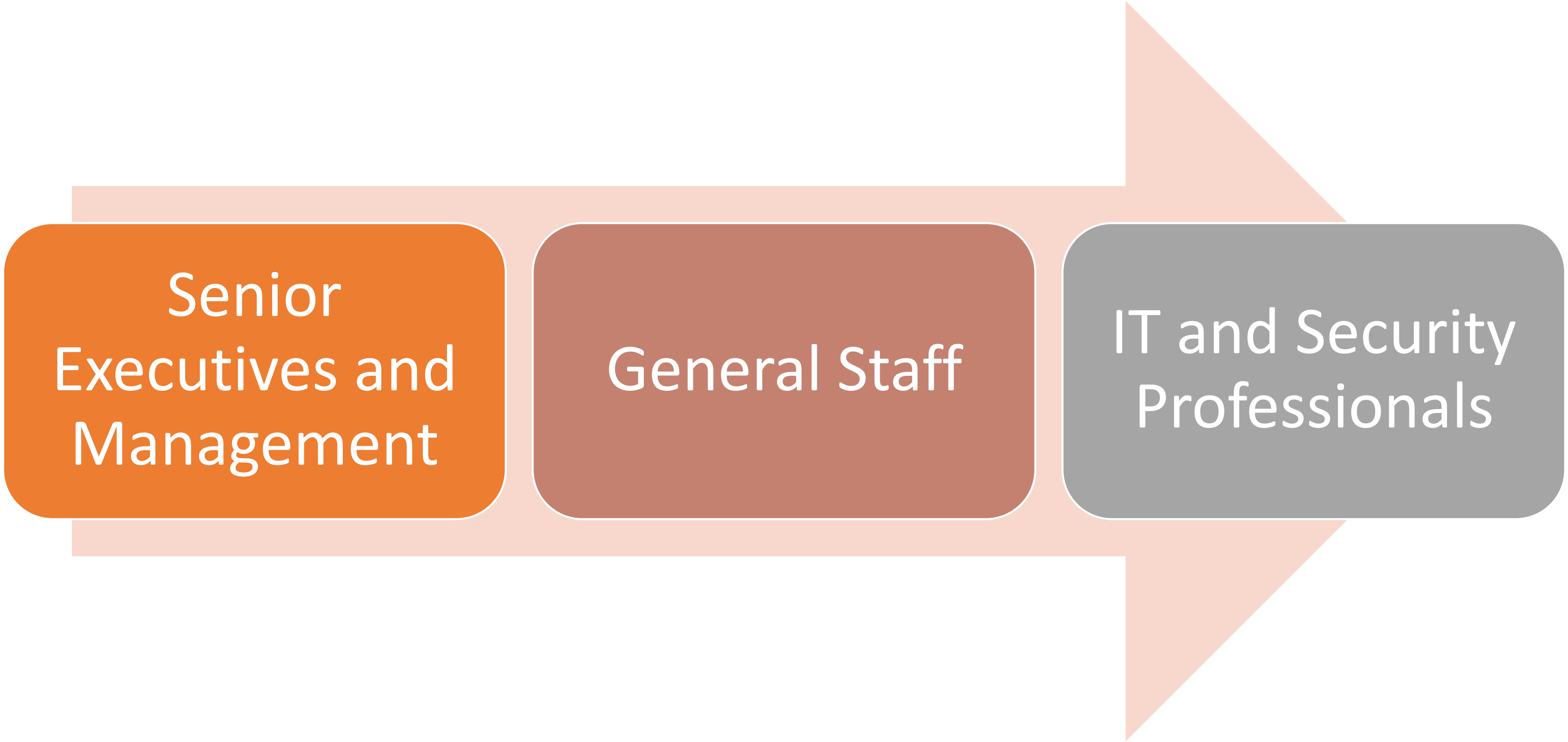
Keep things positive

(not technology)

(everybody is under pressure)

(do not add stress to stress)

Three main populations to consider

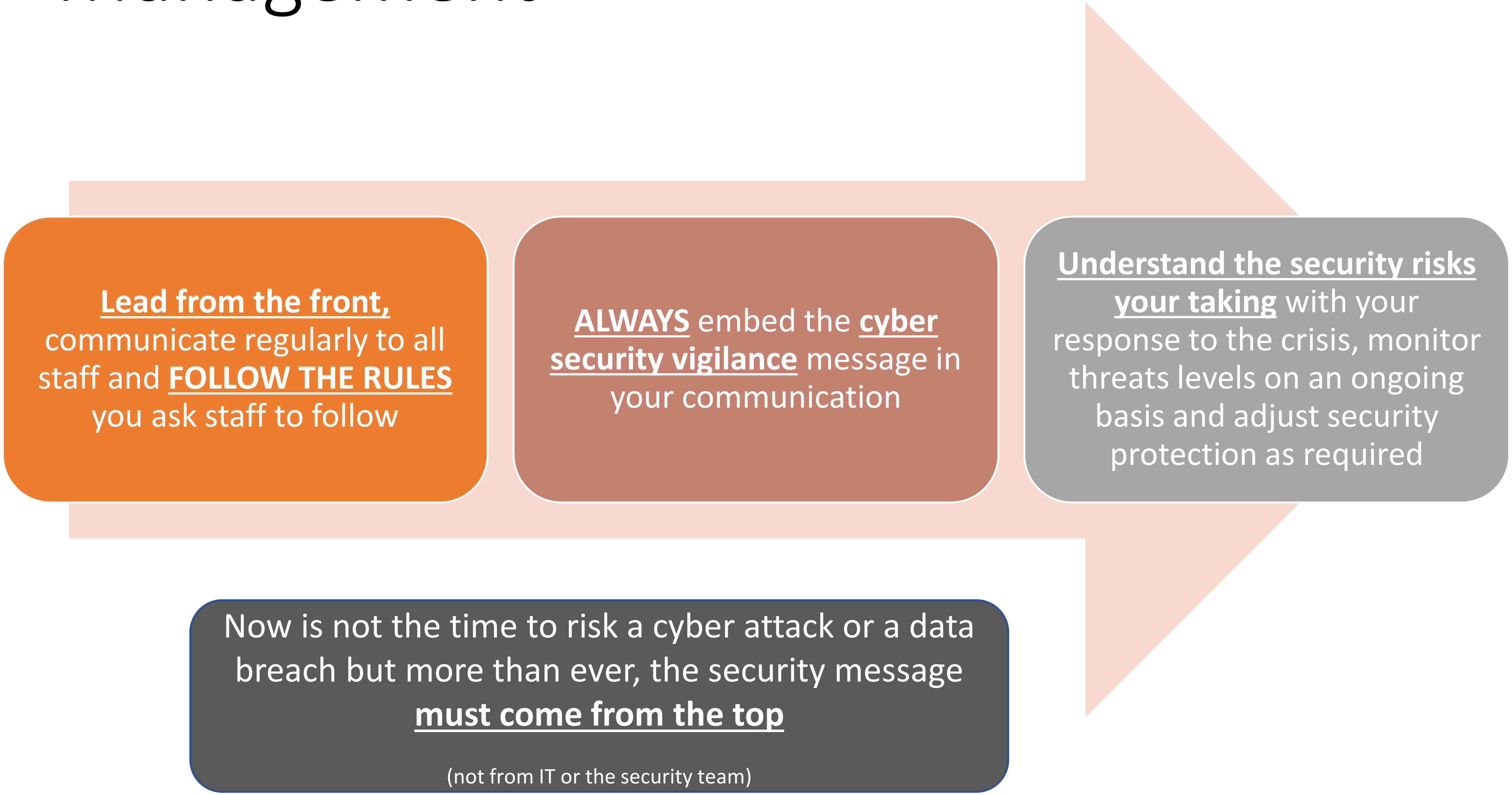


Senior Executives and Management

General Staff

IT and Security Professionals

Key Messages for Senior Executives & Management



Lead from the front, communicate regularly to all staff and **FOLLOW THE RULES** you ask staff to follow

ALWAYS embed the **cyber security vigilance** message in your communication

Understand the security risks your taking with your response to the crisis, monitor threats levels on an ongoing basis and adjust security protection as required

Now is not the time to risk a cyber attack or a data breach but more than ever, the security message **must come from the top**

(not from IT or the security team)

This is not just about scams and phishing emails, but about **embedding a culture of security vigilance** in new working routines at a time of heightened threat

Remote working may be here to stay or even become the "new normal" going forward in some industries

Key Messages for the General Staff

Focus on building **new working routines** which follow corporate and government guidelines and **include breaks**

Be extra vigilant around emails, text messages and instant messages on all platforms (personal and professional)

If in doubt, slow down and **talk to IT & Security** colleagues before rushing into a home made solution

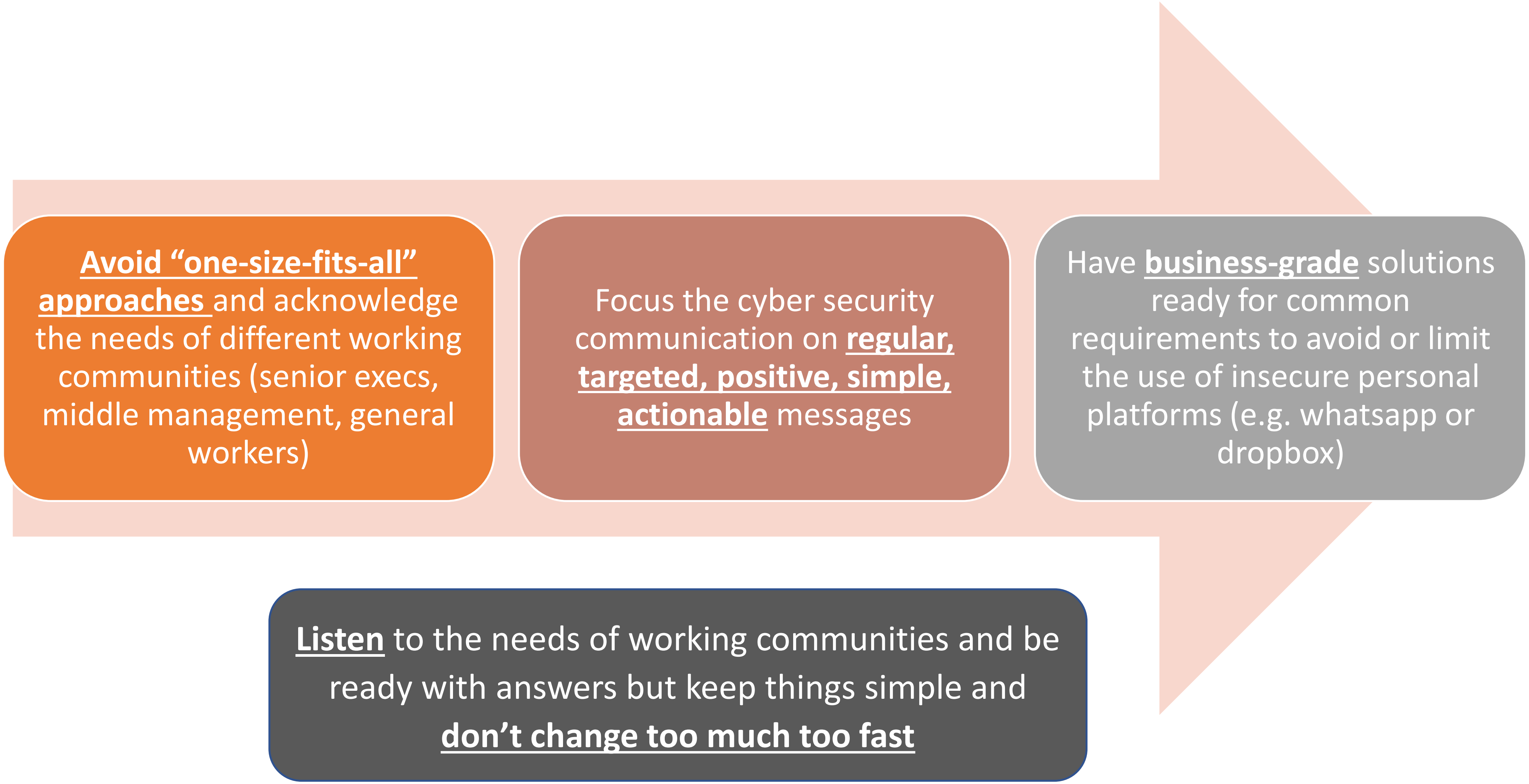
Don’t let stress take over and **don’t cut corners**: There is nothing wrong with asking for help

There will be times where networks are slow or systems don’t work

Personal and professional worlds will collide and the situation could last longer than we expect now

Building new routines is essential to **deal with stress and general mental health**

Key Messages for IT & Security Professionals



Avoid "one-size-fits-all" approaches and acknowledge the needs of different working communities (senior execs, middle management, general workers)

Focus the cyber security communication on **regular, targeted, positive, simple, actionable** messages

Have **business-grade** solutions ready for common requirements to avoid or limit the use of insecure personal platforms (e.g. whatsapp or dropbox)

Listen to the needs of working communities and be ready with answers but keep things simple and **don't change too much too fast**

A positive, simple, actionable cyber security response to the crisis is key to build credibility around the security message and engagement with staff to **avoid the bypass of corporate protective measures**

Focus your messages on simple things people will understand and know how to do

Final Key Points to Consider for IT and Security professionals

- You may have to relax some rules or handle policy exceptions differently to what you were doing before

  - **Stay positive** and do not create more barriers: Everybody is stressed and for many businesses, this is about survival
  - Focus on the **real needs** of the working communities and do not use the opportunity to push your next pet project
  - Think "**defence in layers**": Monitor usage and educate staff, where you cannot prevent insecure practices

- Encourage and drive **separation** of personal and professional computer usage – as much as realistically possible

Examples of practical Do's and Don'ts for IT and Security professionals to consider

DO

Talk to senior executives individually and create a group for them on a **secure messaging platform** (e.g. Signal) so that they can safely share sensitive information

DO

Encourage password protection on sensitive files and **good password hygiene** in general and in particular for file exchanges (through a business-grade platform)

DO

Ask staff to create **different accounts** to separate personal and professional usage on home computers, and educate on physical security and equipment sharing

CONSIDER WITH CARE

Ask staff to reconfigure their home wifi routers

It will be too technical for many and create more stress if it fails

CONSIDER WITH CARE

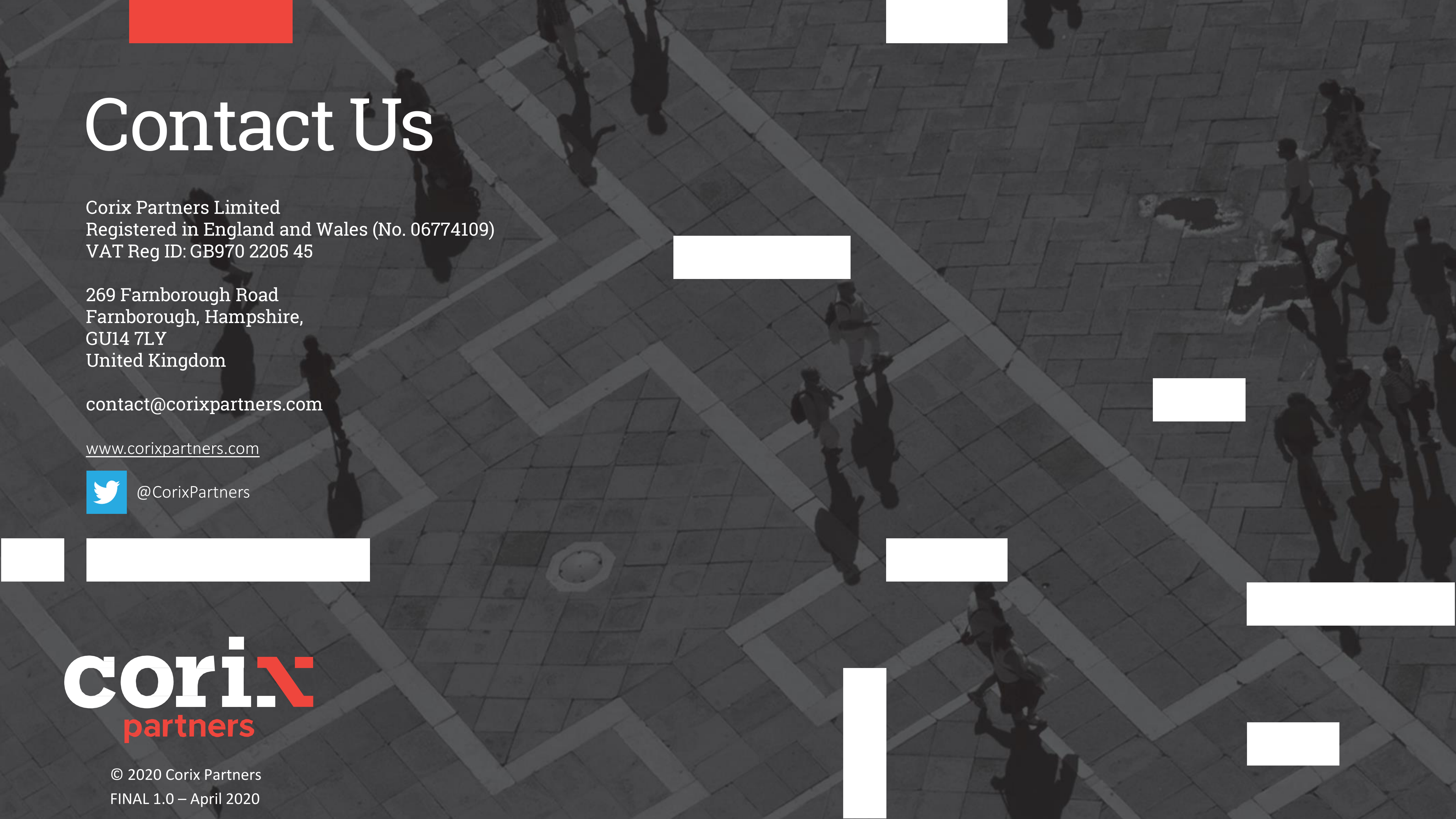
Rush-in the introduction of multi-factor authentication

It could be disruptive and add stress to stress

DON'T

Encourage the professional use of personal emails

They're often shared and insecure



Contact Us

Corix Partners Limited
Registered in England and Wales (No. 06774109)
VAT Reg ID: GB970 2205 45

269 Farnborough Road
Farnborough, Hampshire,
GU14 7LY
United Kingdom

contact@corixpartners.com

www.corixpartners.com

@CorixPartners

FINAL 1.0 – April 2020