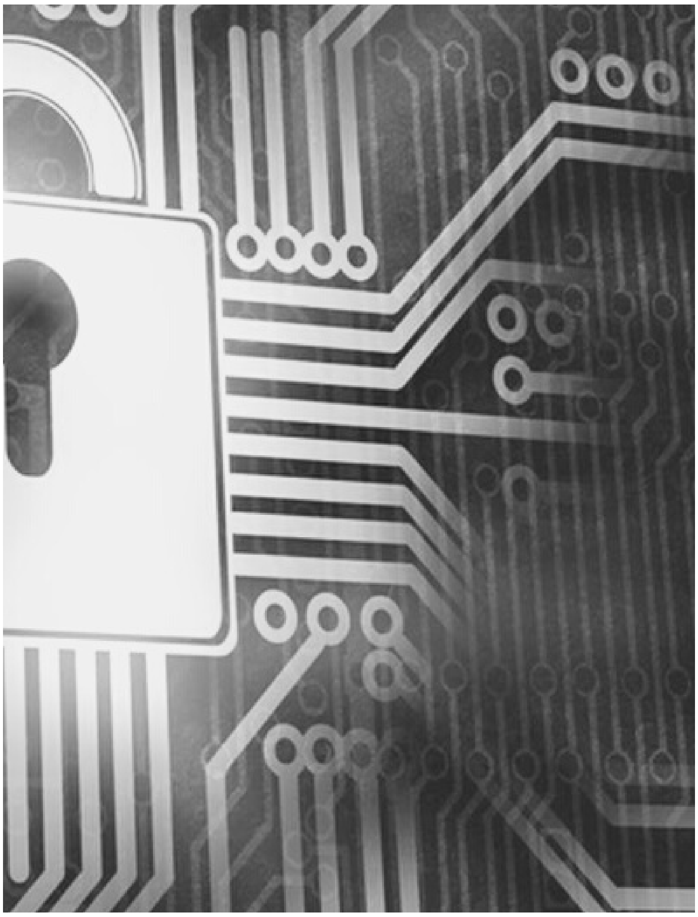
TALK SECURE.

July's Talk Secure promises to be a good one. With the topic of **hybrid working** being hotly debated in the business world we've been looking at it through a security lens. Specifically, have our **security habits changed** and what does this mean for a return to the office?

We've got some fantastic fresh research to share with you too.

- The results from our **hybrid working security habits** survey, and
- Insights from our awesome panel of guests on our recent webinar, '**can security champions aid the transition to a hybrid working model?'**



IN THIS EDITION

The Culture Coach

Security Habits Survey

‘Hybrid Working’ seems set to become a reality for many people, so we launched a survey for non-security people to dig a bit deeper and really gain a true understanding of how peoples’ security habits had changed over the last 18 months. Here are just some of the results and feedback we received.

ONLY 4%
returning to
the office
full-time

- **62% of respondents had no contact from their IT department during the pandemic.** From the first day of working from home, a staggering 62% of people DID NOT have any contact from their IT department to assist and support in their home security set up.
- **60% of people said they used their personal devices for business**. Of those 28% said they always have always done this and 24% told us their use of personal devices for work had increased since working from home.
- A call from a security person to help implement secure practices was one of the most popular ways respondents told us would help them work more effectively at home and at work.

The results of the survey were discussed on our recent webinar, with many amazing points being raised, from defining hybrid working, and making sure everyone knows what it means, to managing subcultures, shadow IT, managing teams and much more. The webinar is on-demand here.

VIEW THE WEBINAR

Keep in touch for the publication of the full report, for now, see some of the key items discussed in the Talking Points...

Talking Points

Should we embrace shadow IT?

For most organisations the move to home working presented a challenge. For some it was bigger than others. Companies that were used to entirely office-based activity (like manufacturing firms) grappled with switching desktops to laptops and obtaining VPN licences in the early days.

What became apparent quickly is, whilst IT might give us the capability to work remotely, people need much more than the tech to be effective. **People need to collaborate.** As the months rolled on people with a passion to keep delivering for their business found new ways of working, new collaboration tools, and inevitably our businesses data got sucked into these tools along with it.

So, what to do? Send out a mandate stopping people? Block everything? Our attendees on the webinar thought probably not. This approach was likely to give rise to the age old saying **'security just stops me from doing anything'.**

A different approach is needed. What we gained through the pandemic is the knowledge that our people are resourceful, creative and want to develop the business. **So, let's use it, not crush it.**

One thought posed on the webinar was, why don't we embrace shadow IT? If done in the right way it:

- Opens the conversation between security and the rest of the business.
- Allows us to research and investigate new technology faster than just one department could do on its own.

The trick is to develop an easy and quick assessment process for new software. That way we are all working together to make sure our business is secure and productive in equal measure.

Can we create a positivity revolution?

We have a term in our industry, FUD, fear uncertainty and doubt. If you've not heard of it before it's when we use big numbers, stats and disaster stories to try and bash the workforce and senior management team into blind panic so they will follow the security rules we set and provide budget. And it was used pretty frequently as a communications strategy throughout the pandemic (outside of security).

However, this type of strategy has short-term effects. If we're talking neuropsychology, FUD gets dealt with in a part of our brain called the limbic system. The limbic system is responsible for our fight, flight or freeze auto-responses. And how each of us respond is very personal and deep-rooted. The global pandemic gave us the opportunity to see this in the extreme:

- **Fight** - the people who took the mantel and tried to make a difference.
- **Flight** - the people who pretended it wasn't happening.
- **Freeze** - the people who were paralysed and scared to do anything.

So, let's think about how this applies to security, and question whether the use of FUD provides any useful strategy for development?

The people on our webinar think it's time to ditch the FUD in favour of the ABCDs, advantages benefits, collaboration (or culture) and development. Why, because when we focus on what's gone right, we can create an image of possibility. Possibility helps us believe that we, individually, can make a difference, and it's infectious we pass it on.

When we stop and actively think about something this type of information, instead of being auto-responded to in our limbic system, is processed in our neocortex, the part of our brain that is involved in higher-order functions such as perception, decision making and language. That means the output is longer lasting, it's meaningful and it's developmental. If we link it to our first talking point around shadow IT it could look like this:

Advantages - how might this new collaboration software people are using put us in a favourable position as a business?

Benefits - what will it mean to the business if we adopt this software?

Collaboration - how do we work together for a win win strategy?

Development - what does the future look like when we are working in this new way?

A challenge for you. Can you flip a typical use of FUD into an ABCD? Share it, see how long it takes to catch on!

Thank you to our panellists and guests on the webinar who, through their comments, suggestions and chatter, helped create the content for these articles.

The Exchange

Name - Steve Mair

Job Title - Principal Consultant

How long have you been within the Cyber Security Sector -? Officially, according to job title and role, around 15 years, but unofficially I've been security minded for my whole career, which is over 30 years. I was writing policies against bringing floppy disks from home and practicing the principle of least privilege as a network manager in the late 80s, so I think it's fair to say I've been in information security all that time. I prefer the term information security because I also consider non-technical aspects such as physical and personnel security rather than "just" cyber.

What keeps you in cyber? What's your passion?

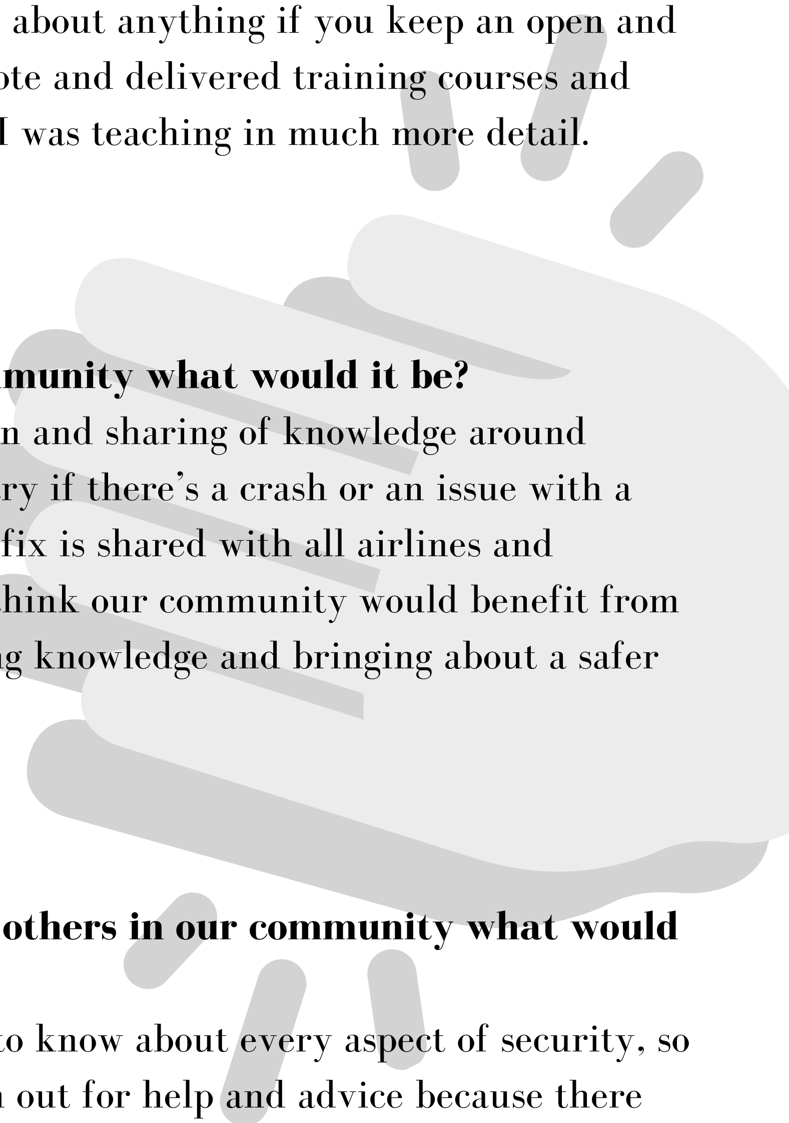
I enjoy working with clients to help them protect their business, organisation and / or citizens: I've worked with clients from sole traders to national governments and, although the scale is different, the principles are the same. The more people who take security seriously, the better protected we all are.

What's been your biggest learning curve?

My whole career! Technology moves so fast, and there are always new developments, that keeping up-to-date is a constant challenge. Given that I started working with technology before the internet and email were common, where TCP/IP was rare and exotic, there's been so much to learn and so much I still have to learn, which is part of the fun and challenge of working in information security. There have been spikes in learning based on job roles e.g., ITIL, Project Management, Security Governance or Cloud Services, but the learning trajectory is always upward.

How do you keep learning?

I listen to a lot of podcasts, attend webinars and watch online content when I can. I also read a lot, not just about security but also about business practices, geopolitics, history: I find that you can learn from just about anything if you keep an open and inquisitive mind. In my previous role I wrote and delivered training courses and that also helped me understand the topics I was teaching in much more detail.



If you were granted 1-wish for our community what would it be?

I would like to see much more collaboration and sharing of knowledge around incidents and threats. In the airline industry if there's a crash or an issue with a particular make and model of a plane, the fix is shared with all airlines and manufacturers so there's no repeat, and I think our community would benefit from a similar approach. It comes back to sharing knowledge and bringing about a safer world as I mentioned earlier.

If you were passing on 1 top tip to help others in our community what would it be?

You can't be expected to know all there is to know about every aspect of security, so don't be afraid to say "I don't know": reach out for help and advice because there are those who will willingly support you if you ask. If you have few contacts, make use of the groups that appear on LinkedIn and other social media platforms, join local cyber forums and attend webinars and conferences - you'll soon identify kindred spirits.

carry on the conversation...

@layer8ltd

layer8ltd.co.uk