a window into cyber

a note from Ben Maidment

BRIT

Life as we know it has changed, and it has brought with it a rapidly changing workplace. As companies around the globe start to move towards a return to the office, many are continuing to incorporate an element of working from home into their 'new normal'. Companies now have the added challenge of a workforce spread between the office, the home office and an irregular commute – each bringing its own cyber security headaches. Communication has therefore never been more important.

In her guest article this month, Dr. Jess Barker looks at the importance of cyber security culture in the workplace and speaks to how CISOs can build a robust one. And for those organisations without a CISO, we highlight Datasafe's plethora of free tools and resources available to support the virtual CISO service all Brit policyholders have.

At Brit, we strive to help you face the future fearlessly. So, although the future of the workplace is still hazy, we're here to provide you with the knowledge and tools to prepare you for anything and the confidence to feel secure.

this month's author: Dr. Jessica Barker

Co-CEO and Head of Socio-Technical Security, Cygenta *@drjessicabarker*

Dr. Jessica Barker is a leader in the human side of cyber security. She has been named one of the top 20 most influential women in cyber security in the UK and has been recognised with a TechWomen50 award. She is the co-founder and co-CEO of Cygenta, where she follows her passion of positively influencing cyber security awareness, behaviours and culture in organisations around the world. Along with being the Chair of ClubCISO, she is a popular keynote speaker who regularly shares her expertise in the media. In 2020, she was the keynote speaker at RSA San Francisco and her book *Confident Cyber Security* publishes this month.

building a cyber security culture

by Dr. Jessica Barker | Read time: 3 minutes

Security has changed over the last few years. As more organisations faced the reality that cyber security is not simply technical but is also inherently about people, we started to see a big shift of emphasis towards security awareness, behaviour and culture.

And then the world changed. With COVID-19, digital transformation plans that were due to take years were implemented overnight. Many organisations had to configure working from home solutions immediately, and lots of technical practicalities had to be tackled. But what does it all mean for cyber security culture? And what is cyber security culture anyway?

security culture in an organisation has a huge impact on everything – from whether people will report suspected phishing emails to the extent to which developers will engage with the security team about a new product they are building.

At the heart of it, culture is how we behave and, more importantly, the beliefs and social norms that underpin why we behave the way that we do. Security culture in an organisation has a huge impact on everything – from whether people will report suspected phishing emails to the extent to which developers will engage with the security team about a new product they are building. Click to watch a video on more about the importance of security culture.

Research we've conducted at ClubCISO has shown that culture has been the number one hot topic for CISOs over the last two years. (Read our reports here.) Now that we're in a state of upheaval, it's hard to know what impact the changes, uncertainty and extra demands of 2020 have had on the security culture of your organisation.

continued on next page

We can refer back to some key elements that we know work when it comes to cyber security culture. We can draw on these to help us navigate this issue even during these trying times:

- Leadership from the top is crucial. Visibly demonstrating best practice cyber security behaviours is one of the most impactful actions that leadership can take to promote a positive culture. How can leadership do this when many people are working from home? A quick video of your CEO discussing the importance of cyber security is a fantastic way of leadership walking the virtual floor.
- In the last few months we have been going to the "pub", having family gatherings and even religious ceremonies – all online. Cyber security awareness-raising that focuses on people's personal (and family) use of technology always has a positive impact. Talking about these issues now has the potential to resonate more than ever.
- At a time when security teams may feel far away from the people they are trying to engage with, establishing a network of security champions throughout the organisation enables security to have much better two-way conversations with the business. What are security champions? They're like fire wardens but for security. They're not experts, but they are familiar faces for people to turn to with issues, inquiries or incidents.

COVID-19 has brought many challenges into our lives, but cyber criminals are seeing it as an opportunity to send more phishing emails and test our defences. Engage with the people in your organisation to make sure they are educated, informed and empowered to be a strong link in security, no matter where they are working from.

an underwriter's outlook

two years on from GDPR:

has it driven growth in cyber security insurance?

Ben Maidment, Class Underwriter – Cyber, Privacy & Technology at Brit Insurance
Read time: 7 minutes

Whilst GDPR has put the spotlight on data privacy and cyber issues, there are other more prominent trends that are driving a greater take-up of cyber insurance.

Many in the industry, myself included, expected the introduction of GDPR in May 2018 to drive a boom in demand for cyber insurance products in the UK and Europe, as data protection and privacy became a board-level conversation for companies both big and small.

However, whilst it has contributed to the growth of the cyber insurance market, we have seen other significant trends drive the real uptick in demand – namely, the exponential rise in size, frequency and sophistication of ransomware attacks and increased understanding of "silent cyber" risks.

click to read full article on IFSEC Global

highlights from Datasafe

BRIT

Datasafe is a free resource for all policyholders to enable them to train their organisations to prevent cyber crime.

This month, take some time to improve your cyber knowledge with the free training available on Datasafe. Ransomware training is a great place to start as almost 2/3 of ransomware attacks are caused by phishing emails, which can easily be prevented. For example, knowing never to click on bad links or attachments sounds easy, but learning to spot them requires training.

get hands on help with Datasafe

Creating and maintaining an employee cyber security training and awareness program can be time-consuming. Datasafe are here to help with a prepaid team to streamline the effort and handle some of the work remotely.

Brit Cyber policyholders receive access to the following free phishing training services:

Interactive online courses covering phishing, business email compromise (spear-phishing), ransomware, and more.

Phishing simulations to identify employees who are susceptible to phishing attacks and deploy targeted training.

Training Coordinator Service that makes it easy for policyholders to implement workforce training and assign courses to employees, along with providing training reports.

recommended Datasafe training courses to start with:

- Phishing
- Employee Mistakes
- Spear-Phishing
- Ransomware
- Threats of a Data Breach
- Malware

how to protect against wire transfer fraud

Wire transfer fraud is when employees are deceived by criminals to wire money to a bank account controlled by the criminals. They often impersonate vendors and other business partners and convince organisations to send them money directly. The most popular warning sign of wire transfer fraud is a request to change an existing wire instruction (e.g. bank account) or a mailing address if payment is by cheque.

3 tips to follow:

Always verify any change to existing wire or payment instructions.

Independently verify the wire transfer request and/or wire instruction changes **by calling a known and trusted phone number.**

Never use the contact information in the original request.