COLLABORATION | INNOVATION
TECHNOLOGY | FORUM

CYBERSECURITY SPECIAL INTEREST GROUP MEETING

On 29 November 2019, the CITF Cybersecurity Special Interest Group (CSSIG) met for its first meeting following the group's launch in September. On the agenda was user education and how members could bring about a cyber risk culture within their organisations.

The group's core message is that cybersecurity is not optional for businesses. We will work to share and exchange information on the relevant issues facing organisations in cybersecurity, and to generate discussion and learn from each other to raise awareness. In so doing, we can all play a part in securing our future through education, awareness and initiating proactive change.

User education faces many challenges in business. This can be a simple emotional obstacle of a lack of interest in employees about cybersecurity. Equally, it can be difficult to develop a simple framing of the complex reality of cybersecurity. And it can be about inertia, a 'not my area' mentality, that regards cybersecurity as something for IT and thereby people stop paying attention.

The CSSIG's desired outcomes for the session:

- To generate ideas about security training to help improve internal company practices.
- To be inspired by other people's ideas – recognising what work works and what doesn't.
- To deepen understanding of the practical implementation of user education.
- To develop ways to better educate users across a global geographic area.
- To bring together ideas about cybersecurity into best practice guide.
- To make cybersecurity more consumable for the sort of people who need to consume it and make the key investment decisions.
- To get users to take the risk seriously.

Report from user education subcommittee

The subcommittee aims to construct a cybersecurity awareness programme, bringing together ideas about creating and measuring successful user education. This could then be taken into user groups on cybersecurity within organisations. Crucially, it is felt that building good behaviours on cybersecurity requires *innovative and multi-channel communication* to make it accessible and engaging for all.

Educating users will, undoubtedly, have challenges. It is not always easy to prove the business case in cybersecurity awareness, making it difficult to get people to support and take part in cybersecurity education – the perception that it is just IT's responsibility. A particular industry issue at the moment are the 'knee-jerk' organisations who will only communicate about cybersecurity when they have a breach.

T +44 (0) 207 052 1894
38 Chancery Lane
London, WC2A 1EN
www.citf.tech

Possible initiatives include posters, newsletters, staff inductions, drop-in sessions and talks addressing tech issues linked to cyber. One extreme way to highlight bad behaviour could be to walk around the office and mark out computers left unlocked when someone is away from their desk.
Measures will be crucial to assess cybersecurity education. There are basic metrics such as number of staff with responsibility for sensitive data, training completion/non-completion, security incidents, avoided breaches, and feedback from staff. Additionally, more advanced metrics could look at organisation threats, reasons employees have not completed training, how to communicate with users of weakness and remote users, improving cyber health of 3rd parties, and identifying security champions.

Solutions to persistent problems:

1. PROBLEM: How to better engage with user feedback.
   SOLUTION: Heat-map of what users want to know, allowing you to directly speak to user needs – combine that with expert opinion
2. PROBLEM: How to make the threats from cyberattacks feel relevant.
   SOLUTION: Link cyberattacks to the brand reputation of the company and give employees business case material that crystallises the threat to the organisation.
3. PROBLEM: Difficulty of raising budget for user education about cyber security.
   SOLUTION: Go back-to-basics – produce evidence to justify costs with metric like work you have done, success stopping attacks, and quantify future threats to the company.
4. PROBLEM: Generational challenges for user education.
   SOLUTION: It is best to approach cybersecurity education uniformly to get the same baseline positive behaviour across the company – then consider specific requirements for different departments.
5. PROBLEM: Users not completing training.
   SOLUTION: One approach could be gamification, creating interactive and graphic interfaces to train employees about cybersecurity. But this will not appeal to everyone, hence the need for multi-channel ways to absorb training information.

Information security education

The fundamentals of education are to make it as easy as possible for users of IT systems to do the right thing. Users should be given information at the right time to prompt the right action, trained to make good decisions, and as a last resort, prevented from doing the wrong thing. But never forget to explain why: respect your users by explaining the rationale behind the cybersecurity rules in language they would understand.

There are range of ways to reinforce good information security behaviour. Regular awareness training is important to shake up inertia amongst employees – make sure the training evolves year on year. Phishing exercises get people having a conversation every few months about spotting phishing emails. Face-to-face threat briefings are another great way to get people to take notice and appreciate the important of the subject matter. ‘Make it real’ by giving a people a sense of who, why, and how; the high level of insight builds trust with those being briefed and draws them into the subject.

Remember that almost no one comes to work with the deliberate intent of committing a security breach. Most stem from lack of awareness, the idea that rules do not apply, or when they complete an unusual task. As a business, you need to take every opportunity to educate your users. The best time to provide prompts or additional guidance is when the user must make a decision – you can use a simple system with a decision tree to help guide the user. Equally, when a preventative control is triggered use that as an educational moment to explain to the user why it happened, and provide a clear path for the user to flag potential false positive

Cybersecurity culture

The internalisation of cybersecurity requires making its behaviours personal. When forging your business' cybersecurity culture, adapt basic good principles to suit your organisation's needs, and remember that cybersecurity culture is about encouraging and not compelling people to change.

> *"An essential part of a company's duty of care to their employees is to help protect them from cyberattacks both at work and at home."*

Try a range of different approaches to leverage cultural shift. Promote the concept of data ownership: whilst IT will help users protect themselves, the ultimate responsibility for securing their data lies with the user. Stress that cybersecurity culture is integral to the brand reputation of the organisation – in the age of GDPR can your company be trusted to protect its data?

Finally, reframe the perception in some businesses that they are not an IT organisation, and so it is not a priority to make cybersecurity part of company culture. The message should always be that an essential part of a company's duty of care to their employees is to help protect them from cyberattacks both at work and at home.

Future actions

The next meeting will be held on 7 February on the topic of board education.

- CITF aims to facilitate subcommittee discussion by helping to organise their meetings – it was noted physical meetings can be coordinated at CITF offices in London.
- Missed outcomes to cover in future: global issues, particularly related to different data rules between countries and how that affects implementing cybersecurity best practice; there will be more discussion on communicating with the board on 7 February.