Panel 1: Deployment of new security practices

Current trends and background context

- Russia's attack on Ukraine has influenced the amount of cybercrime, and this is reflected in trends such as the increase of DDoS attacks.
- The level of cybercrime is rising, partly due to increase in bad actors, but also because it is becoming increasingly easy to access tools that enables this sort of activity.
- As technology has evolved, many layers of programs, code, etc. have accumulated over time, which might explain some of the reasons as to why cyber security solutions have become more complex.

The right attitudes to take when seeking new solutions

- Whether you honestly think you are a likely target or not, it is important to not be complacent.
- Follow strong standards and practices, from strong firewalls to KYC procedures.
- Be proactive, whether that is with training staff, educating yourself on issues relating to cybercrime or keeping yourself updated with the latest trends and issues.

What to do when actively seeking new solutions

- It is very important to not be naïve when exploring what security providers are offering. Whilst there are certainly companies with big reputations, a smaller business may also provide you with what you need. Additionally, outside help (seeking advice, recommendations, etc.) can be very useful when choosing a solution.
- Know what your business is capable of – is there capacity to manage and maintain a security solution yourselves or (especially if you are a smaller company) is outsourcing the way to go?
- Is there a good communication line to tech support when things go wrong, especially if you are outsourcing?
- Be aware of what data would potentially be exposed online, as well as what information is on your own systems.
- Solutions should be, by default, GDPR-ready.

What the business should be doing for the customer

- In terms of making sure that the end user has a hassle-free experience in this domain, the updating of things like hardware and software are massively important. It's a two-way game that applies to both business and customer.
- When it comes to designing the user experience for the customer, this needs to be done in a way that creates the least hassle for them.

Panel 2: Securing data and digital assets

Effective strategies and practices for data protection approaches

- Fundamentally, it is better to have strategies and practices that can do the job satisfactorily rather than absolutely nothing.
- Build a culture internally where everyone should care about the data and that it is secure. Make it easy to care about the data.
- When designing solutions, plan how data security is going to affect a project. Additionally, it is important to consider the life cycle of data, especially with data that exists in cloud systems.
- In general, it is important to see compliance in a business context as opposed to simply thinking about it as simple box-ticking exercise.

Attracting new talent and CISOs

- Awareness and knowledge needs to beyond simply “Where is the server located?”
- Rather than solely relying on recruiting ready-made experts, companies should be more willing to train from within. This can be done in a systematic and productive way where established professionals share as much knowledge as they can with junior members of staff.
- Create more integrated roles where different personal ambitions and talents can be utilised in a new way.

Methodologies and frameworks to apply

- There should be systems/checks in place to keep on top of data management (so that old and potentially unnecessary data isn’t just lying around.) With strong planning and classification practices, this can also make large amounts of data easier to manage.
- For older data, the solutions for discarding this must be easy-to-use.
- Understand what data you need now. Any data that could be useful for future projects can be placed in ‘cold storage’ – hidden from networks.

The human element

- There is a very fine balancing act between making a system incredibly secure whilst also making it easy-to-use for the end user.
- It is important to minimise the number of systems that the end user has to work with. Too many systems with different rules will only increase the likelihood of human error occurring.
- Mandatory password changing must be designed in order to get the end user to create strong passwords when they sign up for an account.
- In order to ensure the end user doesn’t have too much responsibility placed on them, efficient workflows and automation will go a long way.
- Learn from the user. Customers are starting to become more aware of how their data can be used and they will demand that companies have resilient protection practices in place. Their feedback is going to be crucial to developing solutions.