Cybersecurity in the spotlights, from digital new threats to compliance with new demands

Chairman:
John McCarthy
BCS Elite

Facilitator:
Owen Williams
Knight Frank

What we have found!

The key conclusions from the session:

GDPR maturity is very varied driven by a wide variety of factors from the type of business, its customers and the boards' attitude to risk.

- Externally the first indicator to the level of maturity is, has the organisation appointed a DPO? Then, is there a plan with milestones and prioritised risks to be considered for mitigation.
- The priorities generally being around the areas of data breaches and inappropriate use of data where the largest fines would likely apply and where the greatest business risks lie.
- Budget will generally be available to deal with the risks because of the level of the fines that could be applied but if you can find a way of making the required activities revenue generating then it will be easier to obtain the budget.
- We concluded that Cyber security and GDPR do go hand in hand because of the requirement for managing data breaches.

The impact on digital business transformation means that we have to consider product vulnerability, consider protection/defence and deliver and maintain security by design.

- Education and awareness are fundamental and it is necessary to have clear rules, consistent protocols and standards of compliance.
- The desire to decrease the time to market requires the use of a consistent set of tools for security.
- Innovations should be checked carefully for security as they are the most likely place to see little attention being paid to rules.

What we have explored

Among these conclusions, we have developed one of these in greater detail below:

We explored organisational structure, how this varies from organisation to organisation and the variety of structures used to make the boards aware of the issues that arise. We further explored the governance that needs to mature in organisations to ensure that adequate consideration of consideration and mitigation of risks is considered by the right people and doesn't fall though organisational gaps.

What we have left open...

Some questions still remain to be addressed:

- Organisations are generally not GDPR ready and will need to continue to mitigate GDPR risks beyond the GDPR deadline.
- Level of risk, we consider that cyber security is a war to be made up of many battles and we are not confident that this is sufficiently apparent to our broader businesses yet.

Convergences

What points do we share in common:

There was broad agreement across all topics. National infrastructure vulnerabilities were considered the most significant risk because so much depends on them and there was considerable concern that public services were not far enough along the journey to being cyber secure.

Differences

What points do we agree to disagree:

Organisations are different, they have different risks and different customer profiles and this will drive different details in the approaches that need to be taken. But all organisations are at risk.

A picture is worth a thousand words

An illustration that sums up our results:

EVERYTHING IS HACKABLE

NXP