Our Advisory Board is made up of an expert group of global security leaders, who have worked to shape and build the years agenda. Here is an overview of the subject areas, questions and topics they have highlighted for discussion at the summit.

Seeing the attackers' view

- How do they really operate and interact vs. the controls?
- What can we learn from the hacker mindset?

Finance and Budget

- The cost of protecting a business is increasing at scale – businesses are being priced out of the market for many controls
- What are the most effective points to consider when creating the business case for additional budget?
- Is the security budget tangible?
- What are the main issues with 18-month procurement cycles?
- How do you put the money where the "risk" is?

Detection

- Is detection technology fast enough? What's new in this space?

Managing the Board

- How to work with the organisational reluctance to do anything until all evaluation is completed? How do you mitigate this affecting the organisation's ability to move at pace to meet the threat environment changes?
- Willingness to look at new vendors – What's the harm in testing? A testing process enables you to move with the market and environment but how do you mitigate the blocks from organisations in terms of checking suppliers?
- Branding security as a service to the business – persuading not just the board, but the organisation, that security is an enabler.
- What does good governance look like?
- What are the challenges and pitfalls of zero trust?
- Do dashboards make us blind to threats?
- How do you manage the Board's expectations when they are reacting to tabloid stories?
- Business strategy and compliance requirements – how to make them meet in the middle.
- How do you manage the boards limited understanding of security?
- Should organisations insist on cyber awareness training for the board or a member?
- Where should the CISO actually report? Should it be the CIO, or should they be on the board?

Resources

- How do you approach recruitment in the current climate?
- What can you specifically look for to ensure you are recruiting the right team?
- When the available resource isn't there, few business management teams want to slow down with their demands, so what are the strategies to work around this issue?
- Managing offshore recruitment strategies, pitfalls, risks and cultural challenges.

Risk

- Is a rigid mindset slowing things down?
- Cyber risk is not keeping pace with the business and environment. The threat is most likely to be in the future. How do you input tools or methodology for this?
- 'Bulldozing through bullshit' is taking away from important things – how do we stop this cycle?
- CISOs are paranoid and focused on mitigating how do we become more strategic about risk?
- The difficulty in quantifying risk – and communicating it.
- Reputation not loss of records is the integral problem. How do you deal with reputation during and after a breach?
- How do we deal with vendors not meeting compliance requirements?
- The NCSC approach is hazard management, not risk management.
- How many businesses are looking at what is most likely to put them out of business?
- Auditor vs CISO: what's best practice for communicating with an auditor?

DevSecOps

- Automated testing vs testing at the end of the dev cycle?
- Detectify – automating white hat tests
- Full cloud environments – how do they affect the usual dev cycle?

Real vs 'virtual security'

- Compliance checklists vs. 'real security' but a checklist is not up to current security standards.
- Should changes in environment be prioritised over checklists?
- When a majority of questionnaires are pointless, limit resources and don't provide questions relevant to service providing, what's the alternative?

Insider Threat

- A lot of businesses are not prepared for insider threats, particularly with M&As and people exiting the business. 30% of breaches are due to insiders (stats from Verizon research)

Supply Chain

- Client size vs. Business size – SMEs are finding that client security requirements are frequently far beyond the capacity of the organisation to deliver.

- Clients want what we want from suppliers – security. The materiality of risk is substantially changing the whole model of out-sourcing, so what's achievable?
- Vendor security risk – how do you audit vendors that you're bringing in and at what point?
- What is best practice for vendor risk management scoring?
-

Quantifying Cyber Risk/Cyber insurance

- We are unable to articulate a standard or figure, how do we get on the same page?
- How does cyber insurance really work?
- Should cyber insurance auto-force vendors into compliance?

Cyber landscape

- How do we keep up with a constantly changing landscape?
- How do you take all the information and distil it into something meaningful?

Cloud

- Is the on-prem ideal a mirage?
- Speed is a benefit and you can micro-segment, but you can build it quickly and badly which is a security problem. How carefully have you replicated on-prem design?
- Consider – Cloud Security Alliance Standard – is it onerous?