Lunch discussion

What's the problem with cyber?

Colin Robertson, Cyber Director and Lead Ethics Officer, BAE Systems

Thursday 18 January 2018

Colin Robertson, Cyber Director and Lead Ethics Officer at BAE Systems shared his experience of how the company is marrying the two worlds of cyber and ethics in its Applied Intelligence (cyber security) business, identifying a key challenge as skills rather than technology.

This session included:

The company's history

Colin began the session by talking about the ethics conversation in BAE Systems, which focuses on 'how' they conduct their business – as opposed to what they do. He acknowledged that this required accepting the products that the company made and recognising that governments need to defend themselves – a point which some cannot get past.

He also made the point that the company needs to continue to be open about its difficulties in the past, referencing the Woolf Committee and its review, which the leadership at the time committed to implementing in full – a point that was corroborated by Philippa Foster Back, Director of the IBE, who was a member of the Woolf Committee.

How the company manages its ethics

Colin explained the actions BAE Systems has taken to manage its ethics – as a direct consequence of its history. Two of the items discussed were company-wide initiatives; the third was specific for the Applied Intelligence part of the business.

1) Global code of conduct

   The global code of conduct, which is now in its fourth iteration, was explained as the "common currency" for behaviour in the company – whether in the UK, the US, the Middle East or south-east Asia. Having a global document which explains the expected standards of behaviour gives a common baseline and provides confidence to all stakeholders that BAE Systems will act as a responsible business.

   The code is also supported by a flexible, scenario-based, ethics training which is updated annually. It is delivered by managers throughout the business – not the central Ethics team or even local Ethics Officers. To make the training effective, it is supported by manager materials, and the range of scenarios mean that the discussion can be made relevant for the part of the workforce where the training is being delivered. Training on not paying bribes to businessmen in the Middle East will not resonate with an employee who works exclusively coding in Guildford! Colin also acknowledged the limitations of using the title 'Ethics Training' which was often met with resistance in the business. Instead, he hoped that every team would be able to have a good discussion on behaviours that were or were not acceptable, with their manager, at least once a year – and not be aware that they had just done the annual ethics training.

   Colin shared that this infrastructure meant that it was easily possible to challenge behaviours, even remotely or on a conference call, which were not in line with the principles of the code – something that he had done on occasion.

2) Ethics Officer Network

   The Ethics Officer Network in BAE Systems is a group of people in the business who, alongside their 'day jobs', dedicate 15-20% of their time to ethics matters. Colin described his role as the Ethics Officer Network lead in the Applied Intelligence part of BAE Systems. Colin identified the role as an "independent channel" for those in the company who wanted to ask questions or raise concerns, without having to go through their manager – if they felt uncomfortable doing so. In the Applied Intelligence business, Colin is supported in this task by 15-20 others who are able to provide a presence on the ground in all major workforce locations. He admitted to wanting to increase the amount of contact made to the Ethics Officers as an indication that people felt free and willing to speak up.

3) Applied Intelligence Business Conduct Committee
Thirdly, Colin explained the role of the Applied Intelligence Business Conduct Committee, which had been created to help the company respond in an agile way to all new business propositions, which in the cyber security part of the business are much faster moving than in other parts of the company.

Colin described the committee, which is chaired by the General Counsel and included non-executive as well as Ethics Officer input, as a decision-making forum which helps the company meet its responsible trading principles and balance business requirements (for profitability) with making the right decisions.

The committee meets monthly and is an opportunity for the sales team to get approval for their ideas. The committee considers a matrix of risks and is embedded early into the sales process. The focus of the committee is risk based and includes factors such as who the potential customer is, what the proposed capability is and how the customer intends to use it, and the market of the customer. Colin also added that the 'newspaper test' – how will this look as a headline on a national newspaper? – was frequently used in deciding whether to pursue an opportunity.

The committee was described as "having teeth" as over the last four years a significant number of deals – which all would have been profitable for the company – have been turned down on ethical grounds. It was also explained that decisions were only made after "intelligent discussion" directly with the sales team involved and that the committee had a range of actions at its disposal, including the ability to add constraints to contracts.

Challenges

Colin concluded the session by outlining three of the key challenges he saw.

First, he talked about managing risk. In a cyber security business, the understanding of risks is evolving rapidly, and Colin illustrated his point by referring to artificial intelligence, which is a risk area which has just been added as a new category to the Business Conduct Committee risk matrix. He shared the hypothetical example of potential consequences of automating decision-making in a government security analysis centre. The potential benefits of increased processing speed and ability to recognise when a system was under threat were considered, but the question was posed, what if the decision was made autonomously that the most effective solution was to shut down the internet of an entire country? Would this include consideration of the entire critical national infrastructure in the country which would also be affected? How could you quantify the liabilities?

Colin explained that in trying to come to decisions such as this, the Business Conduct Committee attempts to take a holistic view of the situation. The difficulties of this were also shared in the context of would be liable for the insurance in the event of a collision involving a driverless vehicle? The owner of the vehicle? The owner of the driverless software? The car manufacturer?

The second challenged raised involved continual staff engagement. On this point, Colin recognised that the company had a very good tone from the top, but questioned, as many others do, whether all the messages were filtering down through the company.

Finally, Colin addressed the challenge of cultural differences in a company of 84,000 people which operates globally, with an acknowledgement that what works here in the UK cannot necessarily be applied globally. He cited a recent challenge highlighted by the LGBT resources that were available on the company intranet which could not be made available in the Middle East due to a very different legal and cultural position. This example was used to help question how things play out globally. Another example which was shared was between the Danish approach to management feedback – very direct and honest, no holds barred, and that experienced in Asia, where the culture was not to challenge management in an open forum.

Q&A

The presentation was followed by a time of questions from the floor which Colin responded to.