APPG ON CYBER SECURITY MEETING MINUTES 3RD MARCH 2020

Minutes of the meeting 3rd March 2020 at 5.00 p.m. in the Macmillan Room, Portcullis House

Topic:

Aviation Security – keeping the skies safe

Attendees:

Lord Mackenzie of Framwellgate (Chairman)

Lord Arbuthnot of Edrom

Flick Drummond MP

Secretariat:

Prof Keith Mayes – ISG, Royal Holloway

Andrew Henderson – Secretariat APPG

Apologies:

Lord West of Spithead

Rt Hon Sir George Howarth MP

Speakers and comments:

Nicky Keeley, Head of Cyber Security Oversight, CAA – addressed the CAA's Approach to Cyber Security Oversight for UK Civil Aviation

Background
Up until 2018, the CAA was working to understand our regulatory responsibility for cyber security oversight which includes air navigation service providers, airports and airlines through various safety implementing rules. The introduction of the Network & information Systems Regulation[1] in May 2018 [1](with the CAA as co-competent authority) gave a much more substantial requirement for the 11 UK entities that meet the NIS threshold and are deemed Operators of Essential Services. This includes the largest airports, airlines, and air navigation service providers.

It was also clear that the European Commission were minded to include a cyber security element to the aviation security regulations (Reg 300)[2], now published[2] with an implementation date of December 2020. This would bring many more entities into scope for CAA cyber oversight. At the same time EASA (the European Aviation Safety Agency) are also proposing amendments to the aviation safety regulations to further enhance cyber oversight.
The CAA's Approach
Initially the CAA had decided to adopt its own information security assessment (as there was no pre-eminent alternative at the time). The NCSC's then developed the Cyber Assessment Framework, and at the request of our operators of essential services, it was agreed that this should be adopted for aviation. Importantly the CAF is outcome based not prescriptive, so it can be proportionate to risk

[1] http://www.legislation.gov.uk/uksi/2018/506/made

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.246.01.0015.01.ENG&toc=OJ:L:2019:246:TOC

and it also allows bench-marking and comparison with other regulated sectors using the CAF like road, rail and maritime.
It was decided between DfT, NCSC and the CAA that we should evaluate the NCSC CAF to confirm its suitability for aviation and make any essential changes where they were required. This work concluded that there was no real need for substantive changes to the CAF for Aviation[3]3, other than minor formatting changes to make it easier to use.
Whilst this work was underway, it also became clear from the self-assessment returns we had asked from our aviation NIS entities, that there was no clear common understanding of the scope you would apply the self-assessment to, and more work was required to define critical scope in a consistent way across all the entities, whilst recognising that the scope would be variable across the diverse range of aviation businesses.
In considering the governance framework for NIS and broader cyber security oversight, it was decided that the considerable step forward in aviation safety through the adoption of Performance Based Oversight4, should also be applied to cyber security oversight. This placed accountability for performance, and the identification and management of risk firmly in the hands of the entities Board. This is discharged through a board-level Accountable Manager within the entity, who is accountable to the CAA for the entity's performance. This requires rigorous risk management processes to be embedded into the entity's governance processes. Going forward all cyber security oversight will be risk focused and tightly integrated with the CAA's Performance Based Oversight[4].
5 http://publicapps.caa.co.uk/modalapplication.aspx?catid=1&pagetype=65&appid=11&mode=detail&id=9242
Resourcing Cyber Security Oversight
One key strategic decision made early on was that regardless of the regulatory source of cyber security oversight (NIS, aviation safety or security) the CAA would try to apply a single harmonised model[5] to provide greater clarity and transparency to industry. To this end there is one Cyber Team at the CAA who are responsible for all aviation cyber security oversight, this gives industry consistency whilst ensuring we avoid duplication of effort.
It was identified that cyber security expertise was critical to enable effective oversight and it was clear the CAA could not recruit and retain sufficient cyber security experts to run the assurance process at scale in house. In considering our approach to the cyber security role and resourcing, the CAA looked at how other regulators were auditing or assuring their industry. One of the longest standing cyber oversight regimes was the Financial Industry's CBEST scheme overseen by the Bank of England for the UK financial sector, launched in 2016.
The oversight was conducted by 3rd party auditors, who had been accredited under the CREST scheme. CREST is a not-for profit organisation that accredits 3rd party providers of cyber security testing and assurance services. This provided a model for 3rd party oversight under strict rules of accreditation and quality. This is similar to the concept of a "qualified entities" already established within aviation safety regulation. The CAA decided to adopt this model.
However, an evidence gathering exercise took place in the 2nd half of 2018 to ascertain the level of capability of those entities in scope for NIS and this indicated that, in common with many businesses in the UK (and Europe), there was not a high level of maturity. Peter Drissell assumed ExCo responsibility of cyber security oversight in November 2018 and I was recruited as the Head of Cyber Security Oversight shortly after.
Our initial review (in consultation with the NCSC and DfT) identified serious challenges in pursuing the CBEST model. The most problematic issue was that the CBEST model was based on penetration testing of systems with CREST accredited testers as suppliers of this service. Peter likened this to

[3] https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance
[4] https://www.caa.co.uk/Safety-initiatives-and-resources/How-we-regulate/Safety-Plan/Enhancing-CAA-oversight/Performance-based-oversight/

[5] http://publicapps.caa.co.uk/modalapplication.aspx?catid=1&pagetype=65&appid=11&mode=detail&id=9242

assessing Heathrow's overall aviation security plan by use of covert tests alone. Whatever the outcome of these tests, it would tell you little of the airport's overall security performance.
The CAA required accredited 3rd party auditors to review the evidence collected by the entity as part of the CAF self-assessment and provide a validated opinion on whether an entity was meeting the required outcomes.
The team of auditors needed to be expert in cyber security, but importantly not only technically but also expert in audit and risk as well as cyber security in relation to Industrial Control Systems or Operational Technology. Working with DfT and NCSC, the CAA identified the requirements and with CREST we created ASSURE[6]. ASSURE 6launched in January 2020, there are now 8 accredited organisations (including organisations like NCC Group, Context Information Security, Pen Test Partners etc a full list is on the CREST website) and we have 18 applications in progress.

The accreditation scheme model provides an opportunity for regulated organisations to run a tender process or contract with suppliers they may already be utilising for other cyber assurance work, thus making it more cost effective and providing flexibility and choice.

The Cyber Security Oversight Model
The result of all of these considerations was the development of CAP1753 the Cyber Security Oversight model for the aviation sector. This had 4 distinct and complementary elements:
The first element was for the CAA to set a clear exam question for industry. In practice this meant setting very clear criteria for scope (providing a method to identify critical systems consistently by each entity) and adopting the CAF for Aviation as the required assessment framework.
The second element was for the entity to conduct its own due diligence against that exam question and to commission an accredited ASSURE Cyber Supplier to audit the entity's CAF for Aviation and to offer an opinion on its accuracy and validity. This would not involve conducting testing of the entity's cyber security, rather it would be an audit of the evidence provided to confirm that the entity's own assessment of compliance was fully supported.
The third element was for the Accountable Manager to sign off (on behalf of the board) a Statement of Assurance, confirming that the entity had met the requirements of the CAF for Aviation and had identified any significant risk, with suitable mitigations. The completed Statement of Assurance along with the 3rd party ASSURE auditor's opinion will be passed to the CAA, highlighting where significant risks were identified; the mitigations put in place and the proposed corrective action plans to address these risks.
The fourth element, as it currently does in the Safety and Security regulatory environment, the CAA Cyber Team would then address any risk areas directly with the entity as senior decision makers, with a view to resolving any areas of concern. We would expect this process to be entirely collaborative as both the CAA and the entity have the desired outcome of resolving risks and issues that might impact on safety, security or resilience. The CAA will then issue a Letter of Compliance with the cyber security oversight process to the entity.
Should that resolution not be possible, the option remains for the CAA to refer the entity to DfT for potential enforcement action to be taken or for the CAA to act under our safety regulatory powers. We expect this action to be high exceptional, as it is in the safety and security domains.
We are approaching the cyber security oversight process as an incremental process, recognising the need for all stakeholders to build capability and capacity. That said, where the process identifies significant risks, we would expect those to be fixed as they are found.
Timescales for Delivery

[6] https://www.crest-approved.org/assure/index.html

APPG ON CYBER SECURITY MEETING MINUTES 3RD MARCH 2020

We are looking to have achieved completion of the 3rd phase – fully validated plans with the CAA, by the end of October 2020 for NIS operators of essential services. This is a challenging deadline but we, and industry, agree it is achievable if we remain focused on delivery. Over the coming 18 to 24 months we will incrementally increase the scope of cyber security oversight to all applicable regulated entities.

International and National Collaboration

We have consistently challenged ourselves not to reinvent the wheel and instead to look at work that is being done by others, not only because cyber security is cross cutting and we can learn so much from other practices, but also because the entities we regulate will have cyber security risks to manage that will not be aviation specific.

We have also aimed for maximum transparency, publishing our approach and all of the mentioned material online (at www.caa.co.uk) and where we have found a gap, sought to fill it with a solution (like ASSURE) that could be used by many.

Lastly, we recognise that aviation is a system of systems and any international consistency that can be achieved through work with the International Civil Aviation Organisation (ICAO), the European Civil Aviation Council (ECAC) or even the World Economic Forum (who will be piloting the CAF for Aviation this year) will only benefit our industry and the whole aviation system to improve cyber resilience.

I hope that adequately describes the CAA's journey in setting out an effective cyber security oversight model for UK civil aviation, importantly working with aviation to incrementally improve cyber security resilience and capability.

AT – how do the CAA implement regulations across the supply chain?

Do not regulate across the whole supply chain and rely on suppliers working with the sub-contractors and passing regulations down the chain.

KM – asked about ransomware attacks on the aviation industry.

Have introduced methodology for high lighting this, try to make sure that the scope is robust and addresses these types of threats and TTPs. CAA not recently effected by ransomware but aviation as a whole has been hit e.g. Travelex.

GM – regarding the supply chain, this is a key problem area for large firms. How does the trickle down effect work, how can you test suppliers and sub-contractors?

No silver bullet, as part of the guidance given we ask our suppliers to identify their critical suppliers. Important to understand your supply chain and how this works. Important to work with other regulators who control the same actors in the supply chain.

GM - In the maritime sector there are devices that cannot be updated. Do you find this in the aviation sector?

There is work on going to look at this and screening equipment was used as an example. It has a lifetime of 20 years and there are active conversations to bring more of industry together to address concerns jointly. Supply chain do want to come to the table. Important to identify all assets and how to protect them.

RP – What are the limitations of CBEST?

Has expanded quite a lot into C and T BEST and is focussed on penetration testing. CAA's challenge is applying this across their whole eco-system. Not comfortable that they can get a good view.

TH – how does it integrate with business resilience and SENS initiative?

Want to make sure that cyber is not something that takes place in the basement. Ask the business entity to consider and scope activities with all the relevant stakeholders in the organisation. Cited one airline who did this very effectively.

Lee Hannaford, Consultant, Canberra Solutions Ltd

Told the APPG that 18 months ago Gatwick airport was closed for 2 days as a drone had been sighted. 5 agencies tried to control the airport and the loss to the economy was £12m per day. Police were first on scene with snipers.

No legislation in place to provide guidance. No unified command and control as no-one knew who was in control for first 12 hours. Lots of agencies worked hard but not talking to each other. No drone was found and the airport was opened and the cycle happened again. No information was shared.

LH ran a process to review what had happened. No-one was in charge for first 24 hours and each Police force had a different process to follow. No single organisation had OpComs, no single Silver or Gold commander.

Gatwick is packed with technology e.g. cameras, but unable to share the information.

Each service stood up their own Ops Rooms.

When Heathrow was hit, the Army moved in a Rapier battery (seeker not missile) to deal with drones.

No legislation in place to deal with drones. Country has been reactive.

Other problem is data, the information is not there to be used. People are afraid of the Govt holding all our data but Google or FB hold it anyway. If something happens at an airport, that data should be available to be turned into information that can then be presented and utilised (via warrant) by the right people at the right time.

Lots of salesmen turned up to sell systems to take the drones out of the sky without taking into account where it might fall.

Need to manage data so that the Police have the correct information to know legally if someone intends to fly a drone at a location where it could cause disruption. Legislation should be passed to allow data to be gathered to stop drone flying. The correct authorities need access to data, both social and open source so when appropriate, using AI and ML, it can utilise information to make decisions.

When dealing with old firmware, system administrators need to control how devices access the systems – appropriate controls can then be put in place to mitigate risks. Many systems grew too fast such, new technologies added on to old technologies – control was lost, example NHS.

PD – understanding was that COBRA was stood up whilst the Gatwick drone incident happened?

Locally there was no co-ordination. Command and control between Forces needs to tie up better, flow of information needs to be quicker. Command was in place at the strategic level but didn't translate down to the operational or tactical level. No point in having command (leadership) if you don't have control (management).

NK – testing and exercising systems is key. NCSC is doing a lot of work in this regard.

KS – co-ordinating multiple agencies – how do you set it up and who has oversight? Is Parliament equipped to make the legislation.

First question is a challenge, data needs to be protected and not mis-used.

As long as those explaining it to the legislator understand what they are talking about, then it can be explained to the voter. Need to explain what the outcome will be.

Lord Arbuthnot – did not understand part of your solution to this, how would police be aware that someone was going to fly a drone at an airport?

The data exists that show what we do and how we live. Use AI to look at regularities in behaviour or new interests such as a sudden interest in drones. Turn this into a probability that this person is going to commit a crime. Extinction Rebellion announced what they are going to do first and left a data trail about buying a drone and intending to use it. (future session required on random and non-random data, how AI deals with it and how ML makes use of it.)

KS - All drones should have either RFID or GPS

KM – Geo-fencing works with legitimate equipment. It you are up to no good, you can modify equipment. Geo-fencing is useful for someone with malicious intent.

LH – *Not many people with malicious intent. Voters do not understand what geo-fencing means. Collecting data will help to highlight bad behaviour. Need to provide enough layers of the onion to squeeze out bad behaviours*

AT – lots of standards there already. Where is the weak link, in the supply chain? Need to support people and avoid over-legislation.

LH – *if you know the small supplier is a higher risk, you can put different systems in place to work out the risk.*

DP – data piece is important as it links up everything. How do you get the data as a Govt. organisation? Facebook will not let you in.

LH – *challenge to legislate for this. Where there is a marketplace someone will find a way. Data is different than information – its important to understand the difference between the two.*

DP – Not binary, Facebook brings jobs to the UK, the company is about more than data.

NK – data issue is huge. People are still hesitant to share information when it comes to breaches. Must make it more normal to share if there is an incident, no blame games.

LH – *Patriot Act is the US answer to this question.*

GM – not quite as clear cut because GDPR stops US Govt using data on a European individual. GDPR does protect you against the Patriot Act if you are a UK individual, wherever it is held.

GDPR and the Patriot Act are at loggerheads, not yet tested who might win.

Not covered how legally one can take control of a drone, legal aspects not looked at.

LH – *complex to take control of an aircraft. Drones are being built that can be controlled. Main question is the authority to take over a plane. Parliament could look at how a drone can be taken over legally. Trick is to translate this into law.*

AT – Nicky's point about reporting breaches very important. Needs to be more effective.

Kevin Jones, CISO Airbus

Group CISO for Airbus, responsible globally for all Airbus activities. Largest commercial aircraft manufacturer and leading defence player in Europe. In cybersecurity, Airbus has a holistic approach. Vast and global IT estate and protecting that is a challenge.

Industrial controls are a key area for Airbus. Product security is key and has been worked on for decades. People are an important part of cyber security programmes and should not be forgotten. Airbus operates a federated approach to digital security, centrally coordinated with relevant security teams embedded close to where it matters. Co-ordinated centrally using a risk based approach with three areas:

Risk based approach mostly applied to IT.

Regulatory and compliance is met by standards. Work closely with relevant bodies

Two key principles are security by design which is tricky but there is no compromise when it comes to safety critical systems. The other is resilience and testing of this which can be done in different ways. Have one of Europe's leading security evaluation and "red" team capabilities in house.

Consider three elements of the eco-system: people, process and technology. Need them in that order.

Information sharing – member of a number of Information Sharing Groups for aviation and industrial control systems. When it comes to supply chain, have a number of different measures to protect the supply chain. Part of an eco-system which is a traditional approach in the aviation sector - being a good citizen is good for the sector.

Innovation – if we do not innovate, we will have problems in the future so need to look at blue sky development. Interested in how quickly Airbus can transition innovation into the business. Work closely with NCSC on research.

Accelerator in human generated cyber security, first in Europe. Most breaches are allegedly caused by people; but we must turn the human factor into one of the strongest links in an organisational security function. Need to be better with security awareness. Airbus has to work globally across different cultures. Consider the human factor element and make sure that processes are in place.

SM – do you find adequately skilled people to deploy technology and if not how do you find them.

NK – capability is a question that keeps coming up. At an ICAO level there are a lot of questions about keeping staff up to date. Too many courses and not always consistent. Cyber security as it relates to industrial control systems is difficult.

Kevin – *not a simple question to answer. Airbus recruits heavily. Cyber security is not just seen as a technical issue. Wants to offer clear career paths, make it more professionals. Those who manage*

risk and compliance need to understand the technology that they use and the business side. Dealing at Board level is a missing skill.

Real challenge is that industry moves so quickly so keeping technical skills going is tricky. Almost impossible for Universities to keep pace. Many organisations doing training and certification, lots of good training about. Not the be and end all of recruitment.

NK – important to recruit those who want to learn. Just interviewed many people and asked people to name a recent cyber threat and many talked about WannaCry which is now many, many years old.

LH – when it comes to people, the most aware are those between 9 and 18 who do it through culture and not learning. Degree-level teaching does not take into account the world around it. AWS introduce new products very quickly.

People check social media on corporate systems, easy route in to infection.

How many staff know or like their company monitoring them? Education can be personalised by monitoring behaviour and asking appropriate questions such as why do you use TikTok or log onto the free WiFI in the pub.

AT – how do you get the C-Suite to take note of good practices, standards etc. Legislation that makes the C-Suite responsible can help.

Kevin – *be cautious about describing things too closely. CISO at AIRBUS sits outside of IT. CISO should be at highest level of organisation.*

Lord Mackenzie closed the meeting at 18.20.