National Cyber Resilience Leaders Board
Inaugural meeting
Wednesday 7 September 2016

MINUTES

PRESENT: John Swinney MSP, Hugh Aitken, [redacted], [redacted], [redacted], David Ferbrache, Linda Hamilton, [redacted] , Gillian Russell, [redacted], David McNeill, [redacted], [redacted], [redacted], [redacted], Robert Hayes, Louise Macdonald and Anne Moises

APOLOGIES: [redacted], FSB; [redacted], Chair, Education and Skills Workstream.

---

1. Hugh Aitken CBE, Chair of NCRLB, welcomed everyone to the meeting. He explained that the intention will be for this group to meet 2 or 3 times per year, but in order to get solid plans in place from all participants, we may have to meet more frequently for the first year. He expects every participant to commit to leading on an area of action to achieve the strategy outcomes.

2. John Swinney MSP, Deputy First Minister and Cabinet Secretary for Education and Skills, thanked everyone for committing to this exercise. He noted that the strategy is a good start but we all have to increase the commitment and activity rapidly to catch up with the cyber risk. We all need to be alert to this challenge across all sectors. In general we need people to be much more aware, active and committed to improving their own cyber resilience and within their communities too.

He said that cyber opportunities are the focus of our future as a nation and this is an increasing way that citizens connect with government. We have many challenges, for example how do we equip teachers with the knowledge and skills they need, how can we better value and bring in industry expertise into our education sector? Cyber resilience must become routine, not an afterthought. It must be pervasive in all policy areas.

3. David Ferbrache OBE, Cyber Security Director at KPMG, delivered a presentation about the Scottish cyber landscape:

- We need to acknowledge that cybercrime is not the sole domain of hackers, but is driven by ruthless entrepreneurs.
- He explained that the large scale extortion taking place online – ransomware and DDOS attacks – have a supporting criminal economy and a strong social engineering component. Cyber crime in a fast evolving industry.
- We don't have comparable Scottish stats for the extent or impact of cyber crime yet, but we do have for England and wales: cybercrime now makes up 40% of all recorded criminal incidents.
- There is a rapid increase in targeted attacks on CEOs, i.e. masquerading as senior reps in business. This is the largest growing category of fraud. Increasing by 1500% in the last 12 months. $18.5 million in dollars from one private health care provider. Education and awareness are key!

- Bulk data breaches – personal data for fraud purposes and reuse of passwords. Organised crime is spending much more time on linked in.
- How well prepared are Scotland's SMEs? Scotland came out bottom in a survey of SMEs in terms of their cyber resilience preparedness, 19% said they had taken no action.
- Cyber attacks will probably succeed so the bigger issue of about resilience, i.e. planning, response, recovery and maintaining customer confidence. If this happened to your business, how would you respond?
- High end attacks been a wake-up call to the banks, e.g. $951m cyber fraud, $81m was successful! Since then we've seen most global attacks happening on financial sector.
- Getting the basics right (passwords, updates, antivirus) does help with the low end attacks. But the most important thing is education and awareness.

Members engaged in discussions about the content of David's presentation. Key points included:

- Law enforcement – the head of EC3 (Europol's cybercrime centre) was formerly from Police Scotland ([redacted]) and the current force is strongly engaging with the international community. The police are becoming increasingly more active in this area of crime: targeting cyber crime infrastructure and disrupting monetisation output. Gillian Russell mentioned that there is European funding available to support this work.
- Community action – Scotland could be particularly effective in bringing together the financial, telecoms, business, and law sectors to work together. Good initiatives from UK (CISP, National Cyber Security Centre) but sectors in Scotland have the opportunity of working even closer together.
- Profile of business sector – one challenge is that we have more small businesses than larger, so they need to a particular focus of any education and awareness programmes, and for the messages to be specific to the size of business, i.e. small businesses and sole traders have different needs and abilities to medium enterprises.

ACTION: Cyber Resilience Unit to follow up with CBI on awareness raising events/conferences in Scotland. Also to note that [redacted] *(Clydesdale Bank) has had discussions with Hugh Aitken and is happy to be involved in education activity.*
UPDATE: CBI Scotland event 7 December 2016

ACTION: Cyber Resilience Unit to look into the European funding opportunities.
UPDATE: to be followed up

ACTION: Cyber Resilience Unit to prepare short briefing on the purpose of the National Cyber Security Centre and the forthcoming national cyber security strategy.
UPDATE: Brief update at next meeting and fuller briefing to be sent to Board members by end of December 2016.

4. [redacted], Head of Cyber Resilience Policy and Programme, presented an overview of the Cyber Resilience Strategy and current delivery structure. Important to note that Scotland is

focusing on becoming a cyber resilient country, where people can prepare or, withstand, rapidly recover and learn from deliberate attaches or accidental events online. Cyber security relates to the technical measures that can be taken to be safe online. However being safe online goes far beyond just technical measures, it is about behaviours. She highlighted that eight national partners have already produced their action plans for this first year of delivery and expect more to come in over the coming months.

5. Chairs of the current workstreams presented on progress and challenges:

Awareness Raising presented by DSU [redacted]	Key points • We must make full use of all potential partners networks and information routes to convey effective awareness messages to their stakeholders. • Partners are also best placed to convey messages in the best tone and medium for their audiences, e.g. YoungScot using Snapchat in child grooming campaign.
Education, Skills and Professional Development. Presented by [redacted] on behalf of [redacted]	Key points: • This workstream is broken into significant strands as they are distinct and different. A cyber skills group will be brought together soon and [redacted] will chair. Also a cyber resilience learning network to support CPD for teachers/trainers. • The incorporation of cyber resilience into the broader digital programmes is starting to happen in the digital strategy and skills reviews.
Cross Public Sector presented by Anne Moises	Key points: • The CROPS group have met twice including representatives from procurement, have increased membership already and are working to refine actions into achievable goals. • They acknowledge the need to do more awareness activity about board and exec level commitment and understanding. • There is a lot of scope and appetite to embed cyber resilience standards into the audit and supply chain processes so the CROPS group are investigating what 'good' looks like.
Business Enablement presented by [redacted]	Key points • Tier 1 stakeholders already meet quarterly, and this group is fundamental in adopting the communications themes. • Tier 2 stakeholders are currently limited to 6 key membership groups across Scotland who are piloting Cyber Essentials with selected members and sectors (law firms, agriculture, construction and oil and gas).
Research presented by	Key points: • Research is the engine room for cyber security. But this is also an

[redacted] opportunity for academics to make reputation and commercialise innovation.

- There are examples of great cyber security research activity but we're not nationally in a good place. i.e. no Centres of Excellence in cyber security research. We're also under performing in accessing funding and are lacking a cyber security academic cluster. There is a feeling that momentum has been lost.
- However the Scottish Funding Council is starting to map out activity and we're also working with SICSA and SIPR to enable 3 research doctorates as well as funding a coordinator to build research capacity across HE.

Discussion and actions arising from presentations:

- Robert Hayes had some general comments on the strategy – the aspirations in the strategy ("world leaders", "global reputation") won't be achieved by the current programme. He believes that current activity will bring Scotland up to a point where we're in the pack, but it's not where we said we're going to be. If we want to bring people to invest in Scotland then cyber resilience assurance is incredibly important to that. Could the SG provide reputational checking and enhanced security checking? The SME sector are bereft of trusted advisors but overwhelmed with offers of service.
- The group agreed with Robert's points, but the Chair pointed out that initially we need to agree on a timeline of targets and achievability. If we can see a change of cyber resilience behaviour in the SME base then that is a huge win! However the next meeting could include a discussion on future aspirations.
- A couple of presentations touched upon the proposals for a cyber hub in Scotland and what this could look like, how it would aid coordination, clarity or services to improve cyber resilience. Agreed to have further discussion,.
- Also, [redacted] mentioned that we are currently exploring a maturity model which could be used across sectors to determine state of cyber resilience maturity. [redacted] said that Digital Business Excellence Partnership has developed a digital maturity model that he can share. Segmentation is very important.

ACTION – At next NCRLB meeting Robert Hayes to lead a discussion about potential actions to meet strategy aspirations.

ACTION – [redacted] *and Hug will work together to create a compelling narrative for presentations, "44 second elevator pitch" which all Board members (and others) can use. By end of December 2016.*

ACTION – Discussion about Cyber hub concept at next NCRLB meeting. December 2016.

ACTION – [redacted] *to send* [redacted] *link to Digital Maturity Model in the first instance. By 3 October 2016. UPDATE: received.* [redacted] *will give verbal update at December meeting.*

ACTION – Slot on Cyber Hub for next meeting. [redacted] *to prepare.*

UPDATE: this needs to be postponed as we await information on the UK Government funding.

6. Terms of Reference for Board/Commitment of Board Members, led by Hugh Aitken CBE, Chair.

- Discussions focussed on the need for measurable action. Both the First Minister and Deputy First Minister want to see deliverables from all partners, however it was also noted that there is a small financial commitment from Scottish Government compared to the amounts being invested in other parts of the UK. Members noted that they wanted more ministerial leadership, commitment and resources. There is an appetite from private sector to invest in collective activity to make Scotland more cyber resilience.
- Members acknowledge that there is a lot of apathy and lack of awareness from people and businesses. The awareness raising messages are not working and behaviours are not changing.
- It was agreed that government and public sector can strongly influence the business sector through procurement, audit and risk processes.
- Members were interested in using the categories outlined in David Ferbrache's presentation, but all wanted to ensure there was detailed segmentation of audiences to ensure the right messages would be delivered in the right way.

- There was debate around the need to have a more high profile public face of cyber resilience. Should this person be a government minister or independent? We have a lead minister and say the Chief Scientific Adviser - should they step up their profiles in this area or is a separate 'commissioner' type role require?
- Agreed that all ministers need to be able to incorporate cyber resilience messages where appropriate into their portfolios and to be able to speak to their sectors/communities on this risks and opportunities.
- A brief discussion on membership of the group highlighted that there could be better representation from local government. Having representation from the research community was also raised, but agreed that representation would be invited when needed but not a standing membership.

ACTION – All attendees to consider Hugh's ask: "What can you bring to the table?" and email [redacted] *their contributions. By 30 September 2016.*

ACTION - Need to meet before the year end with a view to spanning out with goals, objectives, measures (by quarter, not just annually). It allows us to take this to other communities about how and when we make a difference. [redacted] *to arrange December date in Glasgow. By 5 October 2016.*

ACTION – Further discussions needed to identify a way forward for a 'public face of cyber resilience in Scotland'. All – suggestions to [redacted] *and Hugh by 5 October 2016.*

ACTION – Cyber Resilience Unit to work with ministerial offices and comms teams to identify opportunities to incorporate cyber resilience messages into ministerial engagements. Ongoing.

ACTION – Chair of Communications Group (DSU [redacted]*) to hold a meeting with all working group chairs to discuss how best to coordinate communications actions. By end October 2016.*

ACTION – [redacted] *will follow up a potential member from the local government sector. By end of October 2016.*
UPDATE: Martyn Wallace, Chief Digital Officer, The Improvement Service will join the Board.

National Cyber Resilience Leaders Board
2nd Meeting
Thursday 8 December 2016
Atlantic Quay, Glasgow

MINUTES

PRESENT: Hugh Aitken, [redacted], [redacted], [redacted], David Ferbrache, Linda Hamilton, [redacted], David McNeill, [redacted], Robert Hayes, [redacted], [redacted], [redacted], [redacted], [redacted], [redacted]

APOLOGIES: [redacted], Chair, Education and Skills Workstream; Louise Macdonald, Young Scot; [redacted], SDS; Gillian Russell, SG; Anne Moises, SG

---

1. Hugh Aitken CBE, Chair of NCRLB, welcomed everyone to the meeting. The main purpose of the meeting was to highlight first year progress of the Strategy and reach agreement on the Board's individual and collective actions as we move into year two.

Update on Actions from 1st meeting held on 7 September 2016

2. [redacted] reported progress on actions from the first meeting as follows:-

- Action 1: HA mentioned the successful CBI Scotland Cyber seminar that took place on 7 December 2016. A further two sessions are being planned for next May and Autumn 2017 where further awareness raising activity can take place.

- Action 2: Cyber Resilience Unit (CRU) had no further progress to report re. to European Funding opportunities.

- Action 3: The CRU has provided the Board with a summary report regarding the UK Government's (UKG) National Cyber Security Strategy. [redacted] advised that there will be funding for Scotland from the UK programme in the region of £1.2m per year over the next five years. [redacted] suggested that the Board play a role in determining how best to deliver the strategy's objectives, which also by default support Scotland's own cyber resilience strategy. She proposed the creation of a small group to look at programme funding and priorities for Scotland going forward.

NEW ACTION 1: A working group to be formed to consider priorities for the UK programme . [redacted] ***(UK cyber strategy programme lead - CRU). By end Feb.***

- Action 4: Bob Hayes (BH) would present his thoughts on the characteristics of a cyber nation during the meeting - see below.

- Action 5: Not completed yet. HA advised that the outcome of today's meeting would help determine the narrative required going forward.

- Action 6: [redacted] suggested postponement of discussion on the cyber hub. Focus just now was on expected funding from the UK programme and that the concept of a cyber hub would be included in these discussions, in the light of the role of NCSC.

- Action 7: Digital Maturity Model (DMM)- [redacted] advised that there were different views on what a digital maturity model should look like in relation to cyber and so requested more time to complete this action as there may be an opportunity to influence the Digital Economy Business Survey and work with SG's Digital Transformation Services.

NEW ACTION 2: [redacted] ***to update Board on Maturity Model progress at next meeting.***

- Action 8: As per action 6, discussion on the cyber hub to be postponed.

- Action 9: Workstream chairs and coordinators met to ensure closer working links. These meetings will be informal and will take place roughly quarterly. HA expressed his interest to participate at future meetings which was noted.

- Action 10: [redacted] advised that the CRU have established close relationships with communications teams from SG and other bodies around the preparation of material and key messages. There is also engagement across SG Directorates to align cyber messages within Ministerial briefings and speeches. HA wanted to ascertain the level of formal communication with other Ministers on the cyber agenda. He felt that it was not only the DFM's role to highlight the enormity of the issue but also Mr Mackay's and Mr Brown's. It was agreed to determine an action around the proactive involvement of other Ministers.

NEW ACTION 3: [redacted] ***to work with Chair to consider ways to ensure other key Ministers are proactively involved in communicating positive messages around cyber as part of their respective portfolios.***

- Action 11: [redacted] advised that a meeting of the Communications and Awareness Raising working group took place on 30 November. There was discussion on topical themes and an annual calendar/toolkit of activity that all key partners would be able incorporate into their awareness raising activities was further developed. A further meeting will be convened in January to finalise content and approach. .

- Action 12: [redacted] advised that Martyn Wallace, Chief Digital Officer, The Improvement Service has agreed to join the Board albeit sent his apologies for this meeting.

Overview of first year of the Strategy

3. [redacted] provided an overview of the first year of the strategy and progress. A lot of groundwork has been laid and the workstreams have identified critical pieces activity as we move forward. Highlights from Yr 1:

- Leadership & Partnership: There has been activity involvement to incorporate cyber resilience into other government strategies. This includes the upcoming, refreshed Digital Strategy; the Digital Skills Framework; The Serious Organised Crime Strategy and the Safer Internet Action Plan.

- Communications & Awareness Raising: This workstream has focused on determining key audiences and the right messages. A communications calendar for 2017 has been developed which includes different themes for each month. This is being coordinated in conjunction with Cyber Aware and Get Safe Online. [redacted] also mentioned the recent appointment of a new Scottish Cyber-security Information Sharing Partnership (CiSP) Coordinator, [redacted] to support cyber threat information-sharing.

- Education and Skills: Developments include: inclusion of cyber resilience within the experiences and outcomes of all digital subjects; creation of a Cyber Resilience Learning Network to determine

how to best embed cyber resilience into curricula and into teacher training; mapping of learning programmes available and Action Plans from key partners.

- Research: Given the current lack of sufficient data in Scotland, the CRU has been working with SG Analysts to include cyber-related questions in various national surveys e.g. Scottish Homes Survey and Scottish Crime & Justice Survey. In addition, [redacted] that the Scottish Science Advisory Council (SSAC) will look at cyber resilience risk and future technology developments. [redacted], Prof of Engineering Science, University of Glasgow has agreed to lead this piece of work and SSAC believes SICSA can provide an obvious route to engage the appropriate academics. [redacted], the new SICSA coordinator, has therefore been requested to be involved in this work. David Ferbrache (DF) also offered his support to this work.

NEW ACTION 4: [redacted] ***to link up with DF and*** [redacted]***. By end of January.***

- Business Enablement: The SBRC has been working with a number of business membership organisations. There has been some increase in take-up of the Cyber Essentials scheme through the voucher scheme, led by Scottish Enterprise, albeit there are some difficulties in persuading businesses of the benefits of CE.

- Goods and services: Issues have been raised around trusted partners as there is no single place that businesses in need of cyber assistance can go to, to find a list of cyber security organisations. In January the SBRC will facilitate discussions with Cyber Essentials accredited organisations to begin to tease out how to produce/host a CE assessors and accreditors list and also to work through the challenges of providing a list of organisations who can offer additional assistance in the wide arena of cyber services.

  There are also challenges in attracting and retaining expertise within the cyber goods and services in Scotland as this is a very competitive market and those who can pay well attract the best talent. This is a maturity issue and can only be resolved when the growth of talent in the pipeline is increased along with creating an environment in which Scotland could seek to compete with others in retaining this talent.

- Public sector: The workstream has created a number of sub-groups based on the strategy's priority actions (under Leadership & Partnership) through the leadership of Anne Moises (AM). [redacted] presented a snapshot of results from a recent survey of local authorities (11 in total) and a handful of NHS Health board to understand what cyber security measures are currently in place. Further work on this to follow esp. as it will help inform the development of the maturity model.

Bob Hayes: Characteristics of a cyber nation

4. BH presented his thoughts on what he felt were three key characteristics of any leading cyber nation. He highlighted the following:

i) Presence. Identifying a key figurehead. The Spanish Government has an ambassador who represents their interests globally armed with a clear narrative. Scotland needs to consider whether it needs a public face as well as the message it wants to communicate to the world as a safe and secure place to do business, learn and live.

ii) Coherence. Ideally, leaders across sectors need to own the message which should be consistent and in line with government's own approach.

iii) Walking the walk. What security measures do we want in place? Need to incentivise and encourage the private sector to change behaviours, e.g. sanctions to help change/influence behaviour and identify some quick wins.

5. Following the presentation, [redacted] facilitated a group discussion asking members to contribute their thoughts as well as what needs to be done to achieve a cyber resilient nation. There was clear agreement that Scotland needs to clarify and agree what we are aiming to achieve i.e. whether cyber resilience in itself is sufficient to demonstrate 'world leader' status or do we need a cyber resilience 'plus' approach with its implied cyber-enabled business growth opportunities. **The latter was preferred**. This needs to be articulated as part of a bold, positive narrative. And it would require significant change and investment or all that can be delivered is cyber resilience that is 'just good enough' (like many other countries). A sub-group would be formed to draft such a narrative.

NEW ACTION 5: [redacted]***, BH,*** [redacted] ***and HA to draft a compelling narrative outlining Scotland's ambition on cyber resilience. By end of January.***

NEW ACTION 6: HA to meet with DFM to discuss how to take this forward. By end of February.

6. In seeking to deliver a step change in reducing the 80% of cyber crime that can be prevented by having the cyber basic hygiene in place, it was felt that some definitive actions were required to increase the number of organisations to get the basics right. In a recent KPMG survey, Scottish small businesses were found to be at the bottom of the UK regional list of cyber preparedness. The Board agreed this was a concern for a nation of SME's and with a strategy that had high aspirations around being a cyber resilient, we needed to ensure that SME's become more resilient.

Cyber Essentials is the recognised baseline standard that can be achieved by almost all organisations, irrespective of size. Whilst a Digital Business Excellence Partnership funding initiative has sought to address this by enabling 200 organisations to assess their cyber resilience and achieve the Cyber Essentials Certification, uptake has been slow. SME's are critical components of the supply chain and may present a risk, particularly as the UK embraces the EU General Data Privacy Regulation in April 2018 which will make significant requirements on reporting data privacy breaches and imposing serious fines for failure to protect data.

The Board agreed that compliance with the principles of EU GDPR will set the timescales for the step change that is required and that Cyber Essentials certification will be of value in achieving this.
The group considered that strong leadership is required and that Scottish Government and those within the wider public sector should take the EU GDPR as an opportunity to take a strong stance on backing the Cyber Essentials certification schemes - given the lack of collective endorsement across sectors.

NEW ACTION 7: [redacted]***, AM and*** [redacted] ***to work with HA on developing a narrative on Cyber Essentials. By end of January and in preparation for HA's meeting with DFM.***

NEW ACTION 8: HA to take to Ministers and other Public Sector leads to get high level backing on a statement of support and timelines around the mandation of CE for organisations engaging with public sector to incentivise uptake of this important standard, taking cognisance of EU's GDPR. By end of February (ref. NEW ACTION 7 and 8).

7: Following from the Cyber Essentials discussion [redacted] outlined SG's funding of a dedicated Cybersecurity Information Sharing Partnership Co-ordinator for Scotland, based within SBRC. The Cisp is a secure extranet owned by the National Cyber Security Centre, providing free cyber situational awareness to any business who owns its own IT network. It also enables businesses to engage in sharing threats and

expanding knowledge to allow mitigation against attacks. In addition to this incident reporting and response advice is offered, as well as free organisational network monitoring by the NCSC.

The Board recognised the obvious value of this service, which was not well known within the business community. The Board agreed that funding a co-ordinator was laudable and that more strategic (SG/SE etc) intervention to create the right conditions to get businesses on board the Cisp was needed.

The Chair asked if the group knew how many Scottish businesses managed their own IT to give an indication of the size of the market the Cisp needed to Reach. [redacted] (Scottish Enterprise) agreed to take a task to assess this number. The Chair suggested that as a group we should be bold and set an aspirational figure of on-boarding 10, 000 Scottish businesses to the Cisp during 2017 and agreed to work with [redacted] and [redacted] to discuss the development of an action plan to achieve this.

NEW ACTION 9: [redacted] ***to provide group with an assessment of the number of Scottish organisations who manage their own IT networks. By end of January 2017.***

NEW ACTION 10: Chair to work with [redacted], [redacted] ***and CisP Coordinator to develop and action plan to on-board Scottish Businesses to the CisP in 2017. By end of January.***

NEW ACTION 11: When engaging with DFM, the Chair to recommend that the Scottish Government actively advocate CiSP.

8. BH suggested that the group should consider sending a Scottish rep to report on activity at next year's UK cyber conference in Liverpool in March 2017. Colin Cook's involvement on the Board as Digital lead was suggested esp. given that cyber resilience is to feature as a key outcome of the refreshed Digital strategy next year.

NEW ACTION 12: Gillian Russell (GR)/Linda Hamilton (LH) to invite Colin Cook for Digital membership on NCRLB. By end of January.

NEW ACTION 13: [redacted] ***and communications group to consider how to promote Cyber Essentials and Cisp related communications activity.*** [redacted] ***to produce a single page narrative on both. By end of February.***

NEW ACTION 14: [redacted] ***to consider an appropriate rep at next year's UK cyber conference. By end December.***

<u>Facilitated workstream discussion</u>

8. [redacted] facilitated a plenary discussion around the three key workstreams: Education & Skills; Communications and Business Enablement. Key actions arising from discussion were recorded on flipcharts. CRU to incorporate these into its workstreams' project plans.

NEW ACTION 15: CRU to incorporate agreed actions from this session into team action plan and will engage with individual Board members where appropriate. By end February.

<u>Summing up</u>

9. In summary, the Board agreed on six key areas that they saw as part of the overall step change towards realising our potential:

SCOTLAND AS A CYBER RESILIENT NATION

1. Ministerial commitment. Create the right conditions to meet Scotland's aspirations as a cyber leading nation or, to be content with driving towards a cyber resilient nation where the basics are enough.

Lead: Hugh Aitken

2. Mitigating cyber risk. As a driver for change, Scottish Government and public sector to endorse the Cyber Essentials Accreditation Scheme for organisations wishing to work with them in order to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

Lead: Anne Moises

3. Sharing threat. Rapidly increase the number of Scottish businesses onto the CiSP to improve information sharing and enhanced risk/threat awareness within Scotland.

Lead: [redacted]

4. Embedding cyber resilience into the Digital Strategy. Ensuring that cyber resilience is regarded as the enveloped around all digital developments in Scotland.

Lead: Gillian Russell/Linda Hamilton

5. Scotland-wide coordinated communications activity to ensure coherent and targeted messaging.

Lead: [redacted]

6. **Developing a cyber skills pipeline** for Scotland to ensure Scotland is future-proofed and can have a strong and prosperous place in the cyber security goods and services sector.

Lead: [redacted]

10. HA summed up by thanking everyone for their contribution.

Next meeting: 1st March 2016

National Cyber Resilience Leaders Board (NCRLB)
3rd Meeting
Wednesday 1 March 2017
Atlantic Quay, Glasgow

MINUTES

PRESENT: Hugh Aitken, [redacted], [redacted], [redacted], [redacted], Gillian Russell, [redacted], [redacted], Robert Hayes, Louise Macdonald, [redacted], [redacted], [redacted], [redacted], [redacted] (sub-[redacted] /SDS), Martyn Wallace, Keith Nicholson.

Invited guest: David Robb, Deputy Director, Digital Public Services Division, Scottish Government (in place of Colin Cook, Director, Digital Directorate).

APOLOGIES: [redacted], [redacted], David Ferbrache, [redacted], Linda Hamilton, [redacted], Anne Moises, David McNeill

---

1. Hugh Aitken (HA) CBE, Chair of NCRLB, welcomed everyone to the meeting. Two new members had been invited to join the Board and were in attendance: [redacted], representing the Local Government Digital Office and Keith Nicholson, representing the Scottish Funding Council. In addition to receiving updates on progress from key workstreams, the meeting also focused on developments at UK level and funding requirements of this work.

2. Before updating the Board on actions from the last meeting, the Chair provided an update of his recent telephone call with the Deputy First Minister (DFM). Readout of the key points discussed:

DFM welcomes the work of the Board and recognises the progress made over the past year which is leading to a more cohesive agenda. He fully recognised that cyber resilience sits across a range of different disciplines and elements.

- He has agreed that the Board should scope out what needs to happen – including associate funding - over the next 5 years in order for Scotland to become a leading cyber resilient and capable nation.
- He will attend the May meeting to discuss further.
- He has a firm view on Scotland being a cyber-leading nation, recognising both the threat and the opportunities. He said that our industries and higher education institutions have the expertise to support this.
- He agreed to consider SG leading from the front by introducing Cyber Essentials requirements in our procurement regulations.
- He mentioned that work is being done just now where Police are talking about their long term vision and what the demands on the police will be in years to come.
- He said that there is a significant digital skills shortage and has been talking with SDS on how to improve this. Cyber resilience/security skills is on his radar. In terms of CfE he said that cyber resilience could be an illustration of how the curriculum can be delivered.
- Re. the concept of an Ambassador/Champion for Cyber resilience in Scotland, DFM is supportive of this, however he thinks this should be outside of government (i.e. not a Minister) but and will consider further. Hugh and DFM discussed that it might be a Business Lead Ambassador and Hugh offered CBI to step up and work with SG in leading the charge for Scotland.

Gillian Russell (GR) highlighted the recently launched Policing 2026 public consultation which the Board should consider feeding into given a key aspect of it focuses on enhancing cyber capability. GR also

advised that David Page, Police Scotland's Deputy Chief Officer, could be invited to consult the Board further, if required. As the DFM is attending the next meeting of the Board on 9 May, HA suggested that, in preparation, the Board should come up with specific asks on what is required before presenting to DFM. [redacted] suggested a discussion on this at the next meeting of worktream leads and chairs on 5 April to which other members of the Board are invited, diary permitting.

NEW ACTION 1: Board members and workstream chairs to consider the specific actions and funding requirements at the next meeting of the workstream leads taking place in Atlantic Quay on 5 April.

NEW ACTION 2: Following the 5 April meeting, Cyber Resilience Unit (CRU) to produce a template outlining the deliverables and timelines for specific proposals before presenting to the DFM for consideration ahead of the next Board meeting on 9 May. By 10 April.

NEW ACTION 3: CRU to liaise with Board members to ensure a response from the NCRLB is submitted to the Policing 2026 consultation. CRU to follow up. By 10 April.

4. Some discussion followed in relation to the Cyber Essentials (CE) scheme. [redacted] asked why CE hadn't been raised substantively with the DFM by now. [redacted] advised that this was due to timing; the CRU are still preparing a comprehensive brief on CE to enable the DFM to make a fully informed decision regarding it, and so await official agreement before moving forward. Keith Nicholson (KN) advised the Board to be mindful of the risks in mandating the scheme as it could be perceived as a barrier to SMEs i.e. another 'hurdle' for SMEs participating in the procurement process. This was acknowledged although [redacted] that the Board was only seeking to support – not mandate – across Scotland at this time. Bob Hayes (BH) advised that the principle of supporting a standard (such as CE) was important given the Board's recent commitment towards creating a cyber resilient nation. [redacted] believed there should be move towards mandation albeit tactically and strategically. [redacted] advised that UK Government (DCMS) had offered to have a senior DCMS, NCSC or GCHQ lead to write to the DFM, Perm Sec or Board by way of articulating why CE is to be a flag ship policy and offering encouragement for Scottish support for CE endorsement, if required.

5. The upcoming General Data Protection Regulation (GDPR) (which comes into effect on 25 May 2018) was also raised in this context. It was felt that so far there was limited guidance from the Information Commissioner's Office (ICO) on the awareness aspects. The Board agreed to write a letter to the ICO's office to request such guidance. BH added that Cyber Essentials was useful to start to ensure organisations are prepared for the GDPR as many organisations are setting plans this May to get ready for it.

6. Regarding the earlier point regarding the ambassador, Louise Macdonald (LM) felt it was highly important that this should be someone from the public sector as part of government demonstrating its leadership. This was noted and [redacted] advised that given the different representations on this board, each Board member could provide a suitable narrative around this for their sector. [redacted] agreed to engage on behalf of Scottish Enterprise with the industry leadership groups (ILG) and coordinate a narrative from their perspective. He suggested that industry sectors need to see their sector named in order to draw their attention and turn this into action. [redacted] indicated that the ILG's had been highlighted as key groups to engage on the cyber message but that whilst this had been initiated progress in this area had been slow.

NEW ACTION 4: Board to write to the ICO's office to request guidance on how to promote awareness around the GDPR. CRU to draft on behalf of the Board. By 12 April.

NEW ACTION 5: All Board members to provide a narrative on behalf of their sector. Date dependent on Action 4.

NEW ACTION 6: IB to work with CRU ([redacted] ***) on how best to engage with the ILGs. By 21 April***

Update on Actions from 2nd meeting held on 8 December 2016

7. The Chair reported progress on the action from the second meeting as follows:-

- Action 1: Completed.

- Action 2: Not complete. [redacted] requested postponement of the action until next Board meeting as discussions are still to take place at public sector level as well as with the NCSC who could provide possible in developing a maturity model.

- Action 3: To be completed although [redacted] has begun identifying a number of upcoming Ministerial engagements where key cyber messages can be included.

- Action 4: Complete. [redacted] advised this was about supporting [redacted] as part of his research role.

- Action 5: Complete. [redacted] advised that she would cover the ambition aspect during her presentation that followed.

- Action 6: Complete. As per Chair's update on his recent discussion with the DFM.

- Action 7: Complete. The SBRC have also recently produced a CE Business Benefits document for organisations.

- Action 8: In progress. As advised earlier, CRU are preparing briefing on CE for the DFM although it will not advocate a mandatory approach, in the short term.

- Action 9: Complete. [redacted] advised that there are about 20,000 – 70,000 organisations that manage their own ICT networks

- Action 10: Complete. [redacted] advised that he and the Scottish CiSP coordinator, [redacted], have been working together and have produced a plan on how to engage businesses.

- Action 11: To be completed in April.

- Action 12: David Robb, Deputy Director, Digital Public Services stepped in, in place of Colin Cook (Digital Director, SG) to present an overview of the Digital Strategy Refresh at this meeting.

- Action 13: Complete.

- Action 14: Complete. Some of the CRU team will be attending parts of the upcoming UK Cyber conference.

- Action 14: Complete.

UK Funding Programme

8. [redacted] provided an update to the Board on the proposed funding arrangements being made available to Scotland. There will be £6.5m available over the next four years for transformational cyber-related projects that help to support the implementation of the 2016-2021 UK Strategy in Scotland and, in turn, the Cyber Resilience Strategy. [redacted] advised that closing dates for bids is 24 March. To

encourage sustainability match-funded initiatives would be particularly welcomed. This is an open call to organisations.

9. The board were asked to note that this is not the only source of funding as Scottish Government is working closely with UK Government to identify whether there are any cyber-related projects of interest being taken forward elsewhere via core UKG activity that could be rolled out within Scotland, e.g. Cyber Essentials.

NEW ACTION 7: [redacted] ***to send round call for applications and pro-forma to Board members after the meeting. [Completed)***

Overview of the Digital Strategy Refresh, David Robb, Deputy Director, Digital Public Services

10. David Robb (DR) presented an overview of the Digital Strategy Refresh which is most likely to be published by the end of March. DR advised that, in accordance with Ministerial wishes, the strategy would be a fairly short document with clear actions outlining how Scotland would seize the opportunities of Digital. It was no longer about Scotland's ambitions and is intended to embrace all aspects of society and the economy. DR highlighted that cyber resilience was being introduced as one of the seven key themes in the refreshed strategy. Link to strategy: http://www.gov.scot/Publications/2017/03/7843

11. Comments were invited and HA enquired about the consultation process and Ministerial engagement. DR advised that consultation took place at the end of last year with input from variety of groups. Consensus suggested the need to raise the pace of change in Scotland. DR also advised that a range of Ministers were involved across the different themes but there was more to be done to engage the rest the Cabinet. LM also highlighted the cross-cutting aspects of the refreshed strategy and the fit with Young Scot's 5Rights work which DR acknowledged.

Overview of the National Cyber Security Centre (NCSC), [redacted]

12. [redacted] provided a quick overview of the NCSC which was formally launched on 14 February 2017. [redacted] advised a lot of NCSC's work will focus active defence and will seek to support businesses primarily through-web-based support and the CiSP to engage on sharing threat and intelligence information. [redacted] also advised that the NCSC will be providing assistance to Scotland on incident management procedures in April. HA requested an NCSC rep to be invited to give a presentation at the next meeting on 9 May.

NEW ACTION 8: CRU to invite NCSC rep to the next meeting of the Board.

Business Enablement update, [redacted]

13. [redacted] advised the Board of her discussions with businesses to date as well as updating the group on the SBRC's Scottish Cyber Hub concept. From her discussions with business to date, [redacted] advised that ambition and leadership are emerging as key themes there is a desire to understand what cyber resilience means for them.

[redacted] informed the Boards that she is engaged in three significant discussions around the Hub concept.

- TayCity Deal (Cyber Quarter): The SBRC was working with Abertay University in a £20m bid to create a cyber quarter in Tayside, in which one of the objectives is developing the skills pipeline for cyber security seeking to deliver 50 security graduates to the market and encourage industry to re locate. [redacted] indicated that 12 large private sector organisations have articulated their support and would work with

academia to design the skill sets they require to deliver services thus retaining skills in Scotland. This bid is now through the second phase of the process and [redacted] will update progress at next Board meeting.

- Knowledge Hub: The SBRC Cyber Strategy Group also available as the security Expert Group to the NCRLB have established a short term work group to examine the business needs of the Scottish HUB Concept. 8 Members of the group led by [redacted], accepting the evolving role of the NCSC, have identified a need for a Knowledge Hub. Whilst the sub group had yet to presents its finding to the expert group the following is the vision presented: The creation of a Knowledge Hub which could deliver and integrated Cyber Industrial Community sharing best practice and intelligence to provide enhanced security, monitoring and protection services to business and public customers alike, supported by a strong government enabled education, investment and enterprise framework delivering new ideas and technology, a skilled workforce and business creation, support and growth, appropriate to a strong global market presence.

- Gartcosh Cyber Crime Centre; [redacted] has been asked by Police Scotland senior management to lead an early discussion on the concept of building Scotland's first cyber-crime centre linked to the multi-agency Gartcosh Crime Complex, which would bring together law enforcement, Industry and Academia.

[redacted] also advised the group on her conversation with [redacted] on achieving the aspiration of a Cyber Plus (beyond the resilience basics) which the three initiative she outlined seek to work towards. [redacted] indicated that SE understand how clusters come about on their journey from birth and from the work undertaken by [redacted] the SE Network Integrator it appears that the growth of the cyber goods and services market is looking good and we may be at a tipping point. The question is do we "go big" with investment or not at all? Fintech resilience rests on cyber security proposition which may require a cyber security cluster. IoT may also need this type of support.

HA thanked [redacted] for this update and requested that she keep the Board updated on progress to ensure alignment of activity with the wider strategy direction.

In addition to the above [redacted] referred to the specific asks within the Business Enablement Workstream Update which were specifically in relation to the Boards ability to influence change around the uptake of Cyber Essentials and Cisp.

New Action 9: The Board and the workstreams consider and report on how they intend to promote the Cyber Essentials Scheme standard within their organisations and sphere of influence. The Board members to consult with their own organisations and demonstrating leadership by consider achieving Cyber Essentials Scheme. Board members to send update to [redacted] ***by 19 April.***

New Action 10: The Board and its workstreams consider and report on how they intend to promote the Cybersecurity Information Sharing Partnership within their organisations and sphere of influence. Offer to Board members to invite [redacted]***, Scottish CiSP coordinator, promote the CiSP across sectors. Board members to contact*** [redacted] ***to progress.***

Workstream updates

14. Communications and Awareness Raising: [redacted] asked the Board if any communications-related activity had been undertaken to date. [redacted] advised that Strathclyde University were undertaking similar awareness activity at sector level and on shared-services aspects. LM also suggested referring and linking into the Child Internet Safety Plan which [redacted] is already ware of. [redacted] also added that in relation to the Scottish Government (SG) corporate Cyber Security Strategy, there was a key focus awareness raising around our people and behaviours, and not just the technical aspects. [redacted]

advised this was important because SG was seeking to be more open and share what cyber issues have occurred in-house in order to identify gaps.

15. Public Sector: [redacted] briefly highlighted progress regarding the public sector workstream referring, in particular, to the initial survey that was carried out of local authorities around preparedness. There is a lack of certainty as to the what should happen next and how to go about developing a maturity model. The Board were asked for input. BH acknowledged the difficulty in putting in place suitable maturity model frameworks as they are currently suited to large organisations. He suggested discussing further with ENISA for their advice. Plus, Martyn Wallace, has agreed to assist as part of his link to local government. [redacted] agreed to get a steer from CROPS Cyber members at their next meeting on 9 March.

NEW ACTION 9: [redacted] ***to acquire a steer from CROPS Cyber on the sort of maturity model being sought for the sector. By end March 2017.***

AOB

16. HA asked about how we prepare for the 5-year plan. [redacted] advised that the 5 April workstream leads meeting would be a crucial starting point for drafting the key asks on the key changes we need to see happen in Scotland. HA asked for executive summary to be provided to DFM in advance of the 9 May meeting. GR also suggested that given Brexit, as a leadership group, this Board should consider how our engagement with Europe will look like in future. According GR, there is an opportunity for Scotland to further develop on good relations with Europe.

NEW ACTION 10: [redacted] ***to prepare an executive summary around the key asks from the Board for the DFM in preparation for the 9 May Board meeting. By 13 April 2017***

Next meeting: 9 May 2017, St Andrew's House, Edinburgh

Note of Meeting			
Board Name:	**National Cyber Resilience Leaders Board**		
Date:	Tuesday 9 May 2017	**Time:**	10:00 – 15:00
Venue:	SG, Conference Rooms A & B, St. Andrew's House, Edinburgh, EH1 3DG		

Attendees

Hugh Aitken (Chair), [redacted], [redacted], [redacted], [redacted], Gillian Russell, [redacted], Robert Hayes, Louise Macdonald, [redacted], [redacted], [redacted], [redacted], Martyn Wallace, Keith Nicholson, [redacted] (invited guest), David Ferbrache, [redacted], Anne Moises, [redacted], [redacted], [redacted], [redacted], v

Apologies

[redacted], [redacted] , Linda Hamilton

MINUTES

NO.	ITEM	ACTION OWNER
1.	**WELCOME AND INTRODUCTIONS**	
	Hugh Aitken CBE, Chair of the NCRLB, welcomed everyone to the meeting. Attendees briefly introduced themselves.	
2.	**UPDATE ON ACTIONS FROM PREVIOUS MEETING**	
	An update on key outstanding actions from the last meeting held on 1 March 2017 was as follows:- Action 3: CRU to send link to Board members to invite comments quickly as the consultation on Scottish Policing 2026 strategy has formally closed. Action 4: CRU to follow-up. Letter now drafted to ICO - completed Action 5: Not completed. (Narrative on individual sectors) Action 6: Open action. [redacted] and [redacted] on how to best engage with ILGs Action 7: Completed.UKG Cyber Security Funding 2017-18 Action 8: Not complete. NCSC possibly coming to Sept meet. Action 9: Now integrated into Action Plans.	
3.	**DISCUSSION**	
	GDPR: Short discussion on need for NCLRB to help create consideration for increasing awareness amongst Scottish Businesses despite the ICO UK lead. **HA** suggested a need to created GDPR as a 'burning deck' issue for business and agreed that he should meet with the lead from the ICO to address this. **DF** agreed that business needed a clear road map to follow. MW indicated that with a few exceptions Local authorities had a low understanding of the GDPR risks and were slow adopters.	

	New Action 1: CRU to draft letter on behalf of the Board to the ICO expressing concern about awareness raising (include [redacted]***'s stats) and request a meeting with the ICO (GR and/or HA will meet).***	***CRU – complete***
	New Action 2: CRU will create series of blog articles and guidance around GDPR and NIS Directive and will sign post the top sources of advice and events including sharing resources that Anne's team have created. All partners to share with their communities.	***CRU – complete – toolkit created***
	Digital Maturity Model [redacted] informed the Board that he was meeting with the NCSC lead on this who had been slow in responding but a meeting had been set to discuss the UK position on 11th May. A meeting is also being held on 11th with the NCC Group who are introducing a Cyber Maturity Index into Digital Transformation discussions. [redacted] suggested (later confirmed by **DF**) that the action plan proposal being as presented actually amounts to a Digital Maturity Model in its own right. Action carried forward to next meeting.	
	New Action 3: [redacted]***, DF, AM and MW to collect thoughts on maturity models and formulate a view for the NCRLB by end July.***	[redacted]***, DF, AM, MW - open***
	New Action 4: [redacted] ***suggests selected members of the Board could take action forward on developing the maturity model for both public and private sector.*** [redacted] ***will formalise the baseline standards by July and then AM, MW,*** [redacted] ***and DF will work together to build this into a maturity model (interim in July and finalise in September 2017).***	[redacted]***, DF, AM, MW – now part of AP***
	CiSP and Cyber Essentials update: Only a few responses received from members. CE relevant to measures within action plan for later discussion.	
4.	**PRESENTATION FROM [redacted], KPMG**	
	[redacted] provided an overview of the critical knowledge of Board and staff in delivering a people-centred - rather than technology - approach to cyber security. Commented that internal and external audit had a part to play. It was mentioned that UK DCMS are considering requesting organisations to report on cyber security in annual reports. Spoke of the CBEST Stress Test model used by the financial sector which was very challenging reflective of the level of maturity of financial sector.	
5.	**DISCUSSION ON PRIORITY ACTIONS PAPER**	
	[redacted] set out the intentions of the paper and covered off the first question to the NCRLB. Members discussed what 'realistically' could be achieved and agreed that Scotland was unlikely to be the leader but should strive to be one of the leading nations in CR. [redacted] indicated that countries that were particularly good either had been	

	under direct threat (Estonia) or were very innovative (Israel). **BH** agreed that we need to have a reality check on where Scotland could realistically position itself on a world market. Other comments were as follows: **MW** commented on the need to support intent with appropriate investment. **DF** asked what Scotland had to offer as a differentiator, which he felt was what we should focus on. [redacted] pointed to the Scottish Development International publication suggestion that we have a core skill components and largest technology growth outside London. **HA** advised strategy needs to fit around Scotland's business/organisations not the other way around. Are we failing to attract and retain business in Scotland? If we are then this needs to change and requires leadership from the top. Retraining skilled workforce was also discussed. Differentiator is we are a small enough nations to have the appropriate conversations with those who matte and use influence. As a nation of SME's this should be a focus. [redacted] led a discussion on the Tay City deal and value of securing the Abertay led project. **<u>Public Sector</u>** **BH** argued that this required a light-touch programme management approach with a Senior Responsible Officer. There was general agreement that this was the right approach and that its recognises the need for a proportionality. Several commitments from Board members to onboard organisations they have influence over. Group spoke again of the role of internal audit and external audit through Audit Scotland for public sector. **KN** suggested Audit Scotland did not have sufficient qualified auditors to undertake the task. There was discussion about influencing uptake including through SG letters of guidance and sponsorship to key public sector partners. Suggestion that if there was a will this could be mandated to public sector. **DF** described the proposal as a Maturity Model in its own right which had value if it was implemented. He suggested some consideration around separating the education and awareness issues as a block in their own right as this was an important area to focus on that required some thought and detail. [redacted] informed the Board about work with Scottish Resilience Development Service (SCoRDS) to help bring the issues to life for boards. **<u>Third and Private Sector</u>** [redacted] outlined the proposal in the section which looks to influence a cyber cluster from the third and private sector using appropriate influence levers available. No dissention around the measures which should be similar, if not the same, as the public sector more discussion on the approach and incentives to engage. It was suggested that the third sector should be split from the private	

	and treated as a sector in its own right due to the types of leavers that could be applied. Discussion on numbers proposed. **HA** suggested that CBI Scotland could attract 25 of its members without difficulty. [redacted] suggested that her Expert Group represented some 38 organisations and could be approached along with the Trusted partners scheme of Cyber Essentials certifying bodies to engage. **BH** advised cautioned about providing specific numbers and suggested that the Private Sector would need to be clear what they were signing up to. Discussion then took place in relation to the expectations around drivers and barriers for private sector to engage with the proposal in unregulated areas. [redacted] reiterated that the paper set out the approach in using influence where we had it i.e. through key membership organisations or the top level businesses who could reach out to their supply change. [redacted] indicated that the Industry Leadership Groups which covered 13 sectors managed by Scottish Enterprise were an important set of groups to engage particularly as Ministers chaired a number of these key sectors and the DFM chaired the ILG Chairs group. **DF** outlines his experience of a similar approach with the MOD where organisations were taken on a similar journey initially being asked to sign up to a pledge and then invited to contribute to the setting of the agreed standards. He suggested that perhaps an iterative approach should be considered with some less mature organisations being invited to sign up to a Cyber Pledge which covered the five sections of the action plan thus giving a commitment to go on the journey. Other, more mature, could sign up to the full measures being proposed. [redacted] suggested that it may confuse if we make more than one ask of the sectors; a pledge followed by a commitment to standards. In addition, the GDPR is setting some of the timeframes which is a year away. **AM** suggested that the use of Certificates of Assurance were perhaps lone of many measures of compliance that could be asked for. There was some discussion about those organisations less inclined to participate. **MW** suggested that some form of Badge/Seal of approval may be an idea to incentivise engagement with the action plan. **<u>Learning & Skills</u>** [redacted] outlined the approach in this section and invited [redacted] to cover in more detail and asked members what was missing. [redacted] suggested that retention of skills and creating a talent pipeline was a key consideration. An open discussion ensured over this with a wide set of views being put forward which included: • What's the Differentiator Scotland has? • What are the retraining agenda considerations? • What is our depth of talent? • What are our academic and non-academic routes to talent including tapping self-taught young hacking talent and	

	diverting from crime, hackathon? • Links to the wider digital skills. • What is the talent demand / drain, who measures? • How does FE and HE provision itself to respond? • Employers recruiting across a range of skills for security sector not just those with known cyber security qualifications. • Modern apprentice schemes and on-job training. Need to be clear on what the immediate skills shortages are, as well as the medium and long term issues. High level leadership and direction required from Ministers. **Research & Innovation / Industry** [redacted] and [redacted] outlined the progress made by academic institution in Scotland and the slow but steady growth of the Cyber goods and services market. The UK is heavily funding innovation Centres. Scotland needs to prioritise this if it wants to make a mark. It was suggested that Scotland requires a Cyber Innovation Centre. A discussion then ensued on what could Scotland concentrate on as its niche contribution in which it can make a mark. It was suggested that should concentrate on niche markets such as; • Investment management • Oil and gas • Marine and agriculture **Cross Cutting aspects** [redacted] outlined the approach in this section which included the law enforcement approach. [redacted] informed the group of the Police Scotland 2026 strategy and the cyber strategy that's contained within the thinking. There was some discussion over the confusion caused over where to report crime and the value of Action Fraud to deal with it, and its status in Scotland. It was felt that this is causing confusion for business and required to be addressed. There was a discussion on incident reporting and wider requirement to provide DFM with confidence on managing a scaled and impacting attack on Scotland.	
6.	**ACTION SUMMARY**	
	Action 1: CRU to draft letter on behalf of the Board to the ICO expressing concern about awareness raising (include [redacted]***'s stats) and request a meeting with the ICO (GR and/or HA will meet).*** ***Action 2: CRU will create series of blog articles and guidance around GDPR and NIS Directive and will sign post the top sources of advice and events including sharing resources that Anne's team have created. All partners to share with their communities.*** ***Action 3:*** [redacted]***, DF, AM and MW to collect thoughts on***	***CRU - complete*** ***CRU – complete – toolkit provided*** [redacted]***, DF, AM,***

	maturity models and formulate a view for the NCRLB by end July. ***Action 4:*** [redacted] ***suggests selected members of the Board could take action forward on developing the maturity model for both public and private sector.*** [redacted] ***will formalise the baseline standards by July and then AM, MW,*** [redacted] ***and DF will work together to build this into a maturity model (interim in July and finalise in September 2017).***	***MW – open*** [redacted]***, DF, AM, MW – part of AP***
7.	**DATE OF NEXT MEETING**	
	The Chair thanked everyone for attending. **5 September 2017**, 10am - 3pm, James Watt A, Scottish Government, Atlantic Quay, 150 Broomielaw, Glasgow, G2 8LU	

Note of Meeting			
Board Name:	**National Cyber Resilience Leaders' Board Extraordinary Meeting**		
Date:	Tuesday 16 May 2017	**Time:**	13:30 – 15:00
Venue:	SGoRR, St. Andrew's House, Edinburgh, EH1 3DG or Teleconference		

Attendees

Mr Matheson, Cabinet Secretary for Justice (Chair)
Gillian Russell, Director, Safer Communities

Resilience Division: [redacted], [redacted], [redacted], [redacted], [redacted], [redacted]

Cyber Resilience: [redacted], [redacted], [redacted], [redacted], [redacted], [redacted]

SG Areas: Linda Hamilton, [redacted], [redacted], [redacted], Anne Moises, [redacted]

Police Scotland: [redacted], [redacted]

National Cyber Security Centre (NCSC): [redacted]

External Stakeholders: Hugh Aitken, [redacted], [redacted], Robert Hayes, Martyn Wallace, Keith Nicholson, David Ferbrache, [redacted], Louise Macdonald, David McClure, [redacted], [redacted], David McNeill, [redacted], [redacted]

Apologies

[redacted], [redacted]

MINUTES

NO.	ITEM	ACTION OWNER
1.	**WELCOME AND INTRODUCTIONS**	
	This extraordinary meeting of the NCRLB was opened and chaired by the Cabinet Secretary of Justice, Michael Matheson. The meeting was called following the global ransomware cyber attack on 12 May 2017.	
2.	**PURPOSE AND OUTCOME OF MEETING**	
	Mr Matheson outlined three key purposes of the meeting:- 1. Give a sense of what happened during the ransomware incident and the impact it had across sectors. 2. Share experiences between partners – both the positive aspects and challenges. 3. Reflect on what this incident might mean for the work of NCRLB going forward and establish a process to ensure a lessons process is put in place.	
3.	**BRIEF OVERVIEW OF THREAT**	
	[redacted] from the NCSC provided a brief overview: • First reports of a ransomware attack were received on Friday afternoon and increased over the next 12-24 hours. • 47 NHS Trusts in England (including 27 acute facilities and 5% of Primary Care) as well as 13 NHS Boards in Scotland. • This was an international event which did not specifically focus on or target health services.	

	• The bulk of activity has been around understanding the nature of the attack. There is no confirmation of attribution at this stage. • NCSC has focused on providing advice, guidance and support. • The impact is stabilising and there is no evidence to suggest that a second wave is imminent. • Information exchanges between National Crime Agency and law enforcement were commended. Cab Sec asked [redacted] what engagement with Scottish agencies had been like. [redacted] advised that: • There had been effective interaction between the National Crime Agency (NCA) and Police Scotland. • The NCSC incident management team established direct contact with Scottish Government Resilience and were invited into SGoRR meetings. • Whilst there was bilateral engagement with NHS Digital and CareCERT, he was unable to confirm the level of interaction with Scottish health boards.	
4.	**BRIEF OVERVIEW OF ACTION TAKEN IN SCOTLAND**	
	[redacted] provided an outline of the key activities undertaken in Scotland which included: • Regular SGoRR meetings to coordinate information from all relevant partners. • Effective links and communications with UK Government to share information quickly. • Support and collaboration with NCSC to ensure consistent guidance and advice was shared, and coordinated with affected organisations/bodies. • Contingency plans activated by affected organisations and messages communicated to staff and public. • Preparation of daily Ministerial briefings for media. [redacted] added that links with the NCSC were excellent to aid and share communications. Real time sharing of intelligence through the Cyber-security Information Sharing Partnership (CiSP) initiative demonstrated its value and importance. Through the Scottish CiSP Co-ordinator, we hope to rapidly grow membership of the CiSP going forward.	
5.	**ENGAGEMENT AND AWARENESS RAISING**	
	[redacted] provided an overview regarding public messaging: • The challenges were around the scale across the public sector – over 120 bodies were contacted over the weekend for assurances. This was taken forward successfully. • The focus remained on NCSC as the single source of truth to avoid contradictory advice.	

	• There will still be lessons to improve messaging for the future – this is an opportunity to strike whilst the iron is hot.	
6.	**EARLY REFLECTIONS**	
	[redacted] reported that the banking sector were interested in how quickly advice spread across public and private bodies. SBRC quickly undertook work to communicate with smaller businesses and network groups. Primacy of messaging is an area to consider for future as well as making more effective use of the tech industry in obtaining and sharing information. **HA** reported that there was some correspondence from SMEs asking for direction and messages have been shared. Detailed patching information should be better emphasised and highlighted for the private sector. [redacted] raised the concern that cyber is still largely seen as an issue reserved to IT departments – the message needs to be that cyber and the associated risks are <u>everyone's</u> business. The group agreed with the view that exec and non-exec board members across private and public sectors need to take responsibility and ownership of (cyber) risk. There was recognition that a cultural shift in some areas was required. This was now being considered in the development of training programmes targeted at board level. Mr Matheson agreed that the issue of leadership is a recurring theme that needs to be addressed in future plans. **LM** highlighted use of language/wording in the media during the incident as it could cause undue alarm among the general public. More thoughtful use of language should be considered in future. **LM** also felt this incident was a teachable moment for our young people hence important that we don't lose sight of this learning opportunity. Mr Matheson acknowledged that early comms messages may have gone too far in anticipating the full extent of the incident. There are lessons (UK-wide) around early messages and not escalating the language too early. **MW** suggested that in future we try to use clear and simple language and design templates that everyone can use for common scenarios - which can be exercised and tested.	
7.	**ACTIONS GOING FORWARD: Lessons Identified**	
	Mr Matheson asked how do we establish a process for identifying, taking forward and sharing the lessons from this across public, private, third and academic sectors. The group agreed that there is a role for the NCRLB in this, particularly in coordinating the work already underway in a number of sectors. **HA** drew attention to the fact that the NCRLB have developed an action plan that was to be presented for consideration to the Deputy First Minister at the Board's meeting earlier this month (held on 9 May), however, Mr Swinney was unable to attend due to Parliamentary business. **HA** advised that actions would be taken	

	forward, as planned, but would now be expedited in light of recent events. ***Action 1: HA to draft and share key points from the action plan by the end of the day with Mr Matheson for use in briefings.*** Mr Matheson agreed that this does put us in a more positive position and felt it would be useful to have these points as offered. **KN** said he felt that running exercises in parallel with counter-terrorism (CT) would be beneficial. Mr Matheson agreed and referred to the CT blueprint which includes plans for tabletop exercises with scenario planning. [redacted] highlighted that there is existing expertise within Scottish Government and the Scottish Multi-Agency Resilience Training and Exercising Unit (SMARTEU - responsible for coordinating emergency service training and exercising). This Unit can assist with the debriefing and lessons process. ***Action 2: NCLRB to liaise with SG to establish where they may be able to link in with good practice identified from the CT programme.*** [redacted] advised that Police Scotland had been debriefing this morning so they need to link in with other lessons process in order to share learning. **GR** highlighted the existence of the strategic Scottish Resilience Partnership who are very keen to focus on both CT and Cyber risks, and so can therefore work with the NCRLB to coordinate exercising. **DF** also offered KPMG to undertake a challenge function in supporting the lessons process to help ensure that the real root causes can be identified. This was greatly appreciated by the group - especially as **DF** advised that such support would be 'pro bono'! ***Action point: SG to facilitate and coordinate the lessons process with the NCLRB, Police Scotland and KPMG.***	***HA*** ***NCRLB / SG*** ***SG***
8.	**Assurances**	
	Mr Matheson agreed it was important to highlight the collaboration already taking place and the joint lessons learning process which would help provide public reassurance. [redacted] reiterated the points raised by **HA** in relation to the existence of the NCRLB and the action plan and the need for everyone to take joint responsibility, and look at their own systems to identify what is vital for protection. **HA** reassured Mr Matheson around the short, medium and long term plans including engagement across all sectors and the sharing of best practice.	
9.	**AOB – including any intended media coverage of meeting**	

	[redacted] highlighted that this incident and associated issues are global and the group also need to consider how best to link into learning across the UK, Europe and wider. Mr Matheson thanked everyone for attending the meeting and advised that a note including any action points would issue imminently. Post meeting note - The following news release was issued after the meeting: https://news.gov.scot/news/cyber-resilience	

Note of Meeting			
Board Name:	**National Cyber Resilience Leaders' Board**		
Date:	Monday 10 July 2017	**Time:**	10:00 – 13:00
Venue:	Collins Building, Richmond Street, University of Strathclyde		

Attendees

Board attendees: Hugh Aitken (HA)/Chair, David Ferbrache (DF), [redacted], Bob Hayes (BH), David McNeill (DMcN), [redacted], [redacted], [redacted], Martyn Wallace (MW) Anne Moises (AM), Gillian Russell (GR), [redacted] and [redacted]),

Also in attendance: [redacted] [redacted], [redacted] and [redacted].

Apologies

[redacted], [redacted], [redacted], [redacted], Louise Macdonald, [redacted], Linda Hamilton, [redacted], Keith Nicholson, [redacted], [redacted], Dave McClure and [redacted]. Also [redacted] and [redacted] from CRU.

MINUTES

NO.	ITEM	ACTION OWNER
1.	**WELCOME AND INTRODUCTIONS**	
	Hugh Aitken CBE, Chair of the NCRLB, welcomed everyone to the meeting, with a special welcome to new attendees: [redacted] and [redacted]	
2.	**UPDATE ON ACTIONS FROM PREVIOUS MEETING**	
	An update on outstanding actions from the last meeting held on 9 May 2017 was as follows:- **Action 1**: CRU to draft letter on behalf of the Board to the ICO expressing concern about awareness raising (include [redacted]'s stats) and request a meeting with the ICO ([redacted] and/or HA will meet). • Action complete – the letter will go out on 11 July **Action 2**: CRU will create series of blog articles and guidance around GDPR and NIS Directive and will sign post the top sources of advice and events including sharing resources that Anne's team have created. All partners to share with their communities. • This is included in the Comms Toolkit. Board members to pro-actively use through their comms channels. **Action 3**: [redacted], DF, AM and MW to collect thoughts on maturity models and formulate a view for the NCRLB by end July. • interim view to be given by the end of July; taking on board comments on action plan.	
3.	**DISCUSSION**	

	Draft public sector action plan: HA and [redacted] reported back. Feedback from the Deputy First Minister (DFM) on our approach to public sector has been positive. A consultation period of 6 weeks (beginning at the end of July) will help us better understand the implementation challenges. Finding additional funding for this work is still being discussed. The proposal is for DFM to write out to all public bodies and local authorities on his intention and to publish the action plan in September. There are potential risks relating to the roll-out of Cyber Essentials Plus in local authorities: there's a substantial resourcing issue for such a short timescale, and schools are a huge element in this. The Board felt that: "Aggressive timescales requires aggressive resourcing". A compromise would be to set a target for less complex organisations by March 2018. The Board expressed a desire to have ministerial backing, but also to have some sort of resource and toolkit to help organisations to make these changes. [redacted] offered insight saying that most organisations have about 70% controls in place so it should be a case of helping most of them along for that additional 30%. [redacted] said that there are efforts to embed this activity in the Programme for Government ("PfG") (due for publication in Sept 17). GR pointed out that Ministers will be interested in opportunities for including innovative activity within PfG and Spending Review. NCRLB are asked to propose idea for PfG and SR for a 2 year financial settlement, with up to 3 years for capital spending. ***New Action 1 – <u>NCRLB</u> to propose ideas for PFG and SR (bearing in mind it will be for a 2 year financial settlement, with up to 3 years for capital spending)*** [redacted] mentioned the recent announcement of the creation of a cyber task force by the Australian Government and whether this might be considered for Scotland. ***New Action 2–*** [redacted] ***to follow up links with the Australian Government to obtain more information on its Cyber Resilience Task Force*** **Becoming more proactive in our response to incidents:** BH queried whether our response to the Wannacry attacks was a lost opportunity for proactive/positive comms. HA stated that we need to get a plan in place and signed off so we can be positive and proactive. DF pointed out the meeting coming up on 18 July 2017 to identify lessons learn and identify what to do in future. [redacted] pointed out that Wannacry has increased the awareness and profile of cyber resilience with Ministers,	[redacted] [redacted]

	resulting in a parliamentary debate and cross ministerial agreement on keeping on top of this agenda. HA committed to a heavy message and a "blitz" of activity once the action plan is in place. GR pointed out the need to get action plan right and well positioned; that cross-policy/cross-sector work requires time. **GDPR** HA wants to move faster on GDPR. A huge portion of industry not aware of GDPR – and communication could start about this now as a drip-feed. MHL and MW urged a countdown on GDPR led by the NCRLB. [redacted] suggested this be raised at next Comms sub-group on 20th July. The Board supported this as crucial: to go into the public sector action plan, with a hook and deadline. [redacted] highlighted the reference to GDPR in the comms toolkit. ***New Action 3*:** [redacted] ***and*** [redacted] ***to contact NCRLB members to identify progress of rollout of GDPR comms.*** [redacted] ***mentioned Business Insider's activity in August 2017 about GDPR.*** [redacted] identified plans by FSB to use the toolkit for GDPR; and that Business Gateway are also taking forward activity. [redacted] said Scottish Enterprise are training the staff who are speaking with businesses about this. Key message is that "you can't outsource this issue". [redacted] requested that this message should go higher up in comms toolkit. ***New Action 4:*** [redacted] ***to strengthen GDPR in the Comms Toolkit*** [redacted] mentioned possibility of an emerging shared service for HE for GDPR, similar to the cyber security shared service that exists. [redacted] pointed out that his organisation (Clydesdale Bank) is asking third parties to secure data that they hold; and that they might have to stop work with some third parties who cannot guarantee data. DMcN recommended different levels of messaging for different sizes of organisations; HA suggested collation of regional work; simplify messages; move messages higher. MW suggested a campaign at T- 300 days (29th July). ***New Action 5:*** [redacted] ***to ask comms subgroup what would be possible; NCRLB members to take responsibility for pushing out messages.***	[redacted] [redacted] [redacted] ***and NCRLB***
4.	**Draft position paper and structure of NCRLB**	
	HA asked for initial thoughts on the draft position paper: Members' reflections: positive; a lot of ambition; let's not underplay the things that will let us stand out as a country (not all huge, some quite	

	subtle); good to have an overarching framework that covers the sectors; actions required are well linked to the individuals on the NCRLB. Key questions: How do we ensure we are set up to deliver on the actions proposed in the position paper? [redacted] – Banking Regulator (FCA) bringing retail banks together to discuss Cyber Threats and sharing of information. This included NCSC, National Crime Agency (NCA); would be good to link back to the group via NCSC to ensure we don't duplicate activities. GR identified there will be a range of devolved/reserved issues. DF suggested NCSC be invited to observe on each group. [redacted] raised issue of comms between subgroups. HA gave reassurance that this would be taken care of at board level; [redacted] suggested including co-ordinators (e.g. learning and skills; research, comms, Cisp) across the groups. ***New Action 6: Include coordinators across steering groups where appropriate.*** [redacted] suggested reshaping Research, innovation group as "Innovation and Internationalisation"; RH suggested Industry be called Investment. Four I's (industry, innovation, internationalisation and investment) was suggested. Four Is would align with economic strategy. ***New Action 7: to consider the name for this steering group. (Subsequently proposed "Economic Opportunity")*** DF: does the advice group include advice (and awareness) for general citizens? Digital Participation in SG would include cyber, therefore important that the comms workstream keeps active links with digital participation activity. ***New Action 8: make stronger links between our comms and digital participation*** **Accountability of Board and Steering Groups** BH raised issue of accountability. Is chair of NCRLB accountable to Scottish Ministers? Are board members liable/having FOI liability? Discussion. Board confirmed as advisory, and accountable for an advisory role; Board doesn't have accountability/authority/statutory responsibility. It can drive change, through challenge and support. ***New Action 9: to change from "collectively drive forward the strategy" "advise, challenge and support"*** ***New Action 10: When Mr Swinney signs off the action plans, NCRLB will ask to meet a group of ministers.***	***[redacted]*** [redacted] [redacted] [redacted] /[redacted]

	New Action 11: SG to define the nature of the groups and their governance; also be clear of individual members' roles; terms of reference.	***HA***
	New Action 12: CRU to note request for future discussion about transparency, publication, FOI, conflicts of interest.	[redacted] /[redacted]
	Discussion about reshaping groups: some membership is about knowledge sharing, goodwill, networking. Particular issue for CROPS group as they have certain actions underway. May need to transition these across to the new action plan.	[redacted]
	New Action 13: Anne Moises agreed as chair of public sector group.	
	New Action 14: include GDPR in third sector group's remit. DMcN agreed as convenor of this the group as lead writer of action plan.	***DMcN***
	Private sector: Alignment discussions: need to tidy up aim and terms of reference; need to consider catalyst model in terms of procurement. An expert group has already formed, with 41 big companies on it. Possible model is to split the group into companies (big or small) and representative bodies.	
	New Action 15: [redacted] ***to meet*** [redacted] ***to discuss***	[redacted] ***and*** [redacted]
	New Action 16: [redacted] ***to lead proposal of membership of group.***	[redacted]
	Learning & skills: a multiple group structure: a strategy group, critical friends and a dissemination/knowledge exchange network	
	New Action 17: HA to speak to Damien Yeates about SDS leading the learning and skills strategy group.	***HA***
	New Action 18: [redacted] ***agreed as lead of 4Is group.***	[redacted]
	New Action 19: re advice and expertise group: HA to ask [redacted] ***of Police Scotland if he will chair. Suggestion this group to involve trusted advice bodies, such as Scottish Enterprise. BH happy to support this group, as he leads the cyber working group under the Police Authority.***	***HA***
	New Action 20: [redacted] ***to organise meeting for group leads before next board.***	[redacted]
	New Action 21: Comms & Awareness to be confirmed a function of CRU, servicing all groups.	
	New Action 22: [redacted] ***to send out revised terms of reference for Board and Steering Groups (this will now be by 27 July)***	[redacted]

5.	Action summary	
	1: NCRLB to propose ideas for PFG and SR (bearing in mind it will be for a 2 year financial settlement, with up to 3 years for capital spending). To AD. ***2:*** [redacted] ***to follow up links with the Australian Government to obtain more information on its Cyber Resilience Task Force*** ***3*****:** [redacted] ***and*** [redacted] ***to contact NCRLB members to identify progress of rollout of GDPR comms. MHL mentioned Business Insider's activity in August 2017 about GDPR.*** ***4:*** [redacted] ***to strengthen GDPR in the Comms Toolkit (***[redacted] ***to follow up.*** ***5:*** [redacted] ***to report back on comms subgroup activity on GDPR what would be possible; NCRLB members to take responsibility for pushing out messages.*** ***6: Include coordinators across steering groups where appropriate.*** [redacted] ***to action.*** ***7: to consider the name for this steering group. (Subsequently proposed "Economic Opportunity").*** [redacted] ***/***[redacted] ***/***[redacted] ***/HA*** ***8:*** [redacted] ***make stronger links with SG digital participation*** ***9:*** [redacted] ***/***[redacted] ***to change terms of reference of NCRLB from "collectively drive forward the strategy" "advise, challenge and support"*** ***10: NCRLB to note that when Mr Swinney signs off the action plans, NCRLB will ask to meet a group of ministers. HA.*** ***11:*** [redacted] ***/***[redacted] ***to define the nature of the groups and their governance; also be clear of individual members' roles; terms of reference.*** ***12: HA/***[redacted] ***/***[redacted] ***to note request for future discussion about transparency, publication, FOI, conflicts of interest***. ***13: Anne Moises agreed as chair of public sector group.*** ***14: Include GDPR in third sector group's remit. DMcN agreed as convenor of this the group as lead writer of action plan.*** ***15:*** [redacted] ***to meet*** [redacted] ***to discuss Private Sector Action Plan*** ***16:*** [redacted] ***to lead proposal of membership of Private Sector Steering Group.***	

	17: HA to speak to Damien Yeates about SDS leading the learning and skills strategic steering group and to become member of the Board. ***18:*** [redacted] ***agreed as lead of 4Is /Economic Opportunity steering group*** ***19: re advice and expertise group: HA to ask*** [redacted] ***if he will chair. Suggestion this group to involve trusted advice bodies, such as Scottish Enterprise. BH happy to jointly chair this group, as he leads the cyber working group under the Police Authority.*** ***20:*** [redacted] ***to organise meeting for group Chairs before next Board.*** ***21: Comms & Awareness to be confirmed as a function of CRU, servicing all groups.*** ***22:*** [redacted] ***to send out revised terms of reference for Board and Steering Groups (changed deadline: 27 July)***	
6.	**DATE OF NEXT MEETING**	
	The Chair thanked everyone for attending. **5 September 2017**, 10am - 3pm, James Watt A, Scottish Government, Atlantic Quay, 150 Broomielaw, Glasgow, G2 8LU This will be one more meeting of the existing Board, before the new Board comes into effect. There will also be an opportunity to meet with leads from the Scottish Resilience Partnership and we have invited Ciaran Marting, Head of NCSC provide an update on their plans and priorities.	

Note of Meeting			
Board Name:	**National Cyber Resilience Leaders' Board**		
Date:	Tuesday 5 September 2017	**Time:**	13:00 – 15:00
Venue:	Scottish Government, Atlantic Quay, Glasgow		

Attendees

Board attendees: Hugh Aitken (HA)/Chair, David Ferbrache (DF), [redacted], Bob Hayes (BH), David McNeill (DMcN), Anne Moises (AM), [redacted], Louise Macdonald (LMacD), Keith Nicholson (KN), Damien Yeates (DY)

Also in attendance: [redacted] [redacted] [redacted] [redacted] [redacted], [redacted].

Apologies

[redacted], Gillian Russell and [redacted].

MINUTES

NO.	ITEM	ACTION OWNER
1.	**WELCOME AND INTRODUCTIONS**	
	[redacted] welcomed everyone to the meeting, and advised that Hugh Aitken, Chair of the NCRLB would be joining shortly. Welcome to new members: Damien Yeates, CEO Skills Development Scotland and [redacted], Police Scotland. **Note this meeting is the last meeting of the current Board structure.**	
2.	**UPDATE ON ACTIONS FROM PREVIOUS MEETING**	
	Minutes of the last meeting were approved by [redacted] and BH. An update on outstanding actions from the last meeting held on 10 July 2017 was as follows:- **1: NCRLB to propose ideas for PFG and SR (bearing in mind it will be for a 2 year financial settlement, with up to 3 years for capital spending).** • The Programme for Government was publish on 5 September. Link: http://www.gov.scot/Resource/0052/00524214.pdf Excerpt from PfG relating to cyber resilience: **91** Cyber resilience and security 'Safe, secure and prosperous: a cyber resilience strategy for Scotland' sets out our vision for Scotland to become a world-leading nation in cyber resilience by 2020. The global cyber attack in May 2017, which affected more than 150 countries and had a high-profile impact on some areas of the NHS in Scotland and England, underlined the seriousness of cyber threats. We will ensure the Scottish public sector can cope with threats like this and be a model of cyber resilience. This will involve achieving the National Cyber Security Centre's Cyber Essentials or Cyber Essentials Plus accreditation, providing effective protection against the most common forms of cyber attack. We will work with the private and third	

sectors to develop complementary action plans in order to raise levels of cyber resilience. People are our strongest line of defence. To help them operate safely and confidently in the digital world, we will implement a learning and skills action plan in our education system that instils cyber resilient knowledge, attitudes and behaviours from an early age. We will also ensure our citizens opportunities to develop cyber specialist skills with career paths to help retain talent in Scotland. As the importance of cyber security increases, so do the opportunities for Scottish cyber security businesses to develop and sell products and services across the world. We will work with Scottish Enterprise, ScotlandIS and other partners to implement an economic action plan to support new ideas and cutting-edge research through collaboration.

2: [redacted] **to follow up links with the Australian Government to obtain more information on its Cyber Resilience Task Force**

- [redacted] has contacted the Australian Government and we hope to have more information on this in the next few weeks. [redacted] and [redacted] to follow up. Link to taskforce info: https://www.pmc.gov.au/cyber-security/cyber-resilience-taskforce

3**:** [redacted] **and** [redacted] **to contact NCRLB members to identify progress of rollout of GDPR comms. MHL mentioned Business Insider's activity in August 2017 about GDPR.**

- [redacted] and [redacted] developed a light-touch tool kit which was sent to Board Members to pass on to their comms teams. This has been updated slightly and KJ will send the revised version to all users. CRU are also putting out 2 – 3 messages on GDPR per day on SG social media channels.

4: [redacted] **to strengthen GDPR in the Comms Toolkit (**[redacted] **to follow up.**

- As above

5: [redacted] **to report back on comms subgroup activity on GDPR what would be possible; NCRLB members to take responsibility for pushing out messages.**

- [redacted] gave an update on this as an agenda item.

6: Include coordinators across steering groups where appropriate. [redacted] **to action.**

- This is now in place.

7: to consider the name for this steering group. (Subsequently proposed "Economic Opportunity"). [redacted] **/**[redacted] **/**[redacted] **/HA** Action Plan's name remains "Economic Opportunity"

	8: [redacted] **make stronger links with SG digital participation** • There is now security and resilience advice on Digital websites. [redacted] has also spent time with our Digital colleagues ensuring they are aware of the projects we support. **9:** [redacted] **/**[redacted] **to change terms of reference of NCRLB from "collectively drive forward the strategy" "advise, challenge and support"** • This has been done. **10: NCRLB to note that when Mr Swinney signs off the action plans, NCRLB will ask to meet a group of ministers. HA.** • [redacted] will arrange for meetings with Mr Swinney and NCRLB leads when action plans have been finalised. HA met with Mr Swinney re. the launch of the public sector action plan (Nov) **11:** [redacted] **/**[redacted] **to define the nature of the groups and their governance; also be clear of individual members' roles; terms of reference.** • Terms of Reference have been sent out to group leaders and are awaiting comment. [redacted] mentioned that the conflict of interest matter will require careful consideration and sensitive management. **12: HA/**[redacted] [redacted] **to note request for future discussion about transparency, publication, FOI, conflicts of interest.** • This has been done. **13: Anne Moises agreed as chair of public sector group.** • This has been done **14: Include GDPR in third sector group's remit. DMcN agreed as convenor of this the group as lead writer of action plan.** • GDPR has been included. **15:** [redacted] **to meet** [redacted] **to discuss Private Sector Action Plan** • This has been done by telephone. **16:** [redacted] **to lead proposal of membership of Private Sector Steering Group.** • [redacted] has written to 18 organisation of varying sizes, and all are very keen to participate. She will also invite the private sector members from the old structure Board including [redacted] (Conoco-Philips), [redacted] (Clydesdale Bank), and [redacted] (Commissum). **17: HA to speak to Damien Yeates (DY) about SDS leading the learning and skills strategic steering group and to become member of the Board.** • This has been done. Gordon McGuinness will lead the Learning and Skills strategic group (with Louise Macdonald as vice chair),	

	and DY will be the Board Member. **18:** [redacted] **agreed as lead of Economic Opportunity steering group** **19: re advice and expertise group: HA to ask** [redacted] **if he will chair. Suggestion this group to involve trusted advice bodies, such as Scottish Enterprise. BH happy to jointly chair this group, as he leads the cyber working group under the Police Authority.** • [redacted] has agreed to co-chair this group with BH **20:** [redacted] **to organise meeting for group Chairs before next Board.** • [redacted] will do this some time in Oct/Nov. • Meeting arranged for December 5. **21: Comms & Awareness to be confirmed as a function of CRU, servicing all groups.** • This has been done **22:** [redacted] **to send out revised terms of reference for Board and Steering Groups (changed deadline: 27 July)** • This has been done	
3.	**Action plan timeline**	
	[redacted] talked through a draft timeline. There was some discussion on interdependencies across the plans and how this would be reflected and managed with regard to the order of completion. [redacted] said that she will set up working sessions with the action plan leads to address this. ***New Action 1 –*** [redacted] ***to arrange working sessions with action plan leads in October to discuss interdependencies and timelines.***	[redacted]
4.	**Governance restructure:**	
	HA joined the meeting and explained that the aim of the restructure was to bring more focus to the work of the Board, and to reduce the number required to attend Board Meetings. HA expressed the view that the proposed structure was just about right, but that he was open to suggestion or critique. He also stressed the need to progress actions with quality and speed. [redacted] explained that the aim of this agenda item was to get Board agreement on the proposed structure as well as the terms of reference. With regard to the frequency of meetings, [redacted] explained that the Board would meet 4 times a year, but that action plan leaders may meet at other times to progress their specific tasks and the CRU can support this.	

	There was some discussion on the importance of comms across all of the action plans, and this is reflected in the proposed structure, with comms spanning the work of all 6 steering groups. DY and LMacD called for comprehensive comms plans for strategic messaging, critical incident messaging, and integrated comms for the 6 priority areas - this was discussed further in the Comms and Engagement agenda item. [redacted] asked Board Members for agreement on the proposed Board structure - this was agreed. [redacted] asked Board Members for agreement on the proposed terms of reference – this was also agreed.	
5.	**Engagement, Comms & awareness raising**	
	[redacted] explained that because of the importance of communications across all of the steering group action plans, communications had been considered as a separate group, however it was quickly identified that a communications plan could not be devised independently of the other action plans, and before knowing what the contents of those plans would be. A comms plan for each of the priority areas will be developed side by side with the action plan. In the meantime [redacted] and [redacted] have been building relationships with the relevant comms contacts in sector groups as they will have a role in raising awareness among their own stakeholders. There was some discussion on communications resourcing, and [redacted] advised that there will be an element of reliance on stakeholders comms to disseminate messages. DY, LMacD and DMcN advised that Board Members need to take responsibility to ensure messaging is shared throughout their own networks. Board members offered their own comms leads to support this work and[redacted] /[redacted] to make contact. ***New Action 2:*** [redacted] ***/***[redacted] ***to engage with Board members' comms leads to arrange comms plans for each workstream*** HA suggested that the CBI event on 8 November should be an annual one, and that there should also be events throughout the year and added that CBI would be happy to help support that. DY asked whether there would be one umbrella campaign which would go out to everyone. [redacted] advised that there was already a wealth of trusted campaigns and advice available, and there was no desire to duplicate any of that – which is why NCRLB has not carried out a campaign before. It is likely that the action plan for Systems of Support and Guidance will deal with the range of information currently available, and the full set of action plans will identify what still needs to be done.	[redacted] [redacted]

	[redacted] pointed out that what is needed is a mechanism to get communications out when incidents happen. CiSP is one platform, but the issue is wider than that and a plan is not yet fully developed. As a result of discussion, it was identified that 3 sets of comms plans were required; A comms plan for the strategy; A plan for crisis comms; and A set of integrated comms plans for the priority areas/workstreams. ***New Action 3 –*** [redacted] ***and***[redacted] ***to develop comms plans for the strategy, for crisis comms, and for integrated comms for the priority areas*** [redacted] mentioned that the Cross-sector Safety & Security Communications (**CSSC**) hub will be an excellent route out to mass messaging. There will be a bulletin on cyber awareness for Cyber Resilience week and thereafter they will work with the NCRLB to decide on the planned approach to ongoing communication. There was some discussion around cross party awareness. [redacted] advised that a letter on the Public Sector Action Plan consultation had been sent to the Rural Economy and Connectivity Committee but that she would look into further cross party awareness. ***New Action 4 – [redacted] to look into cross party awareness. [redacted] to support HA to consider how to reach cross party cyber leads***	[redacted] ***/***[redacted] ***[redacted] & HA***
6.	**Board's Position Paper**	
	HA asked Board Members if they were content with the proposed Position Paper. There were no objections or comments, and the position paper was agreed. ***New Action 5 – HA will send the paper to the Deputy First Minister (DFM)*** ***New Action 6 – [redacted] will work with HA to arrange a meeting with DFM***	***HA*** ***[redacted] & HA***
7.	**Update on Action Plans**	
	Public Sector The DFM has written to all public body CEOs for their views on the public sector action plan. Responses are due by 15 September. The 20 already received are broadly positive, but carry concerns around responsibilities and economy of scale. When the consultation period has closed, comments will be collated, cyber catalyst organisations will be identified, and any proposed changes to the action plan will be considered. An increase on CiSP uptake has already been seen, and CRU are working	

	with colleagues in Procurement to include Cyber Essentials as an advisory element of the procurement process. **Advice, Support and Response** [redacted] joint Chair advised that he and Bob Hayes (BH), joint Chair were keen to conduct a gap analysis around the foundation of evidence, and to move on to delivery following that. [redacted] explained that he is the Chair of the Management Board at the Crime Campus and is doing work with [redacted] and the private sector around the creation of a Cyber Hub. This group is keen to get ahead with plans for the Hub. [redacted] stressed the effectiveness of agencies with shared common aims working together, and that a response across private and public sectors, in line with the approach to other major resilience incidents, is the way forward. LMacD asked for reassurance that the action plan for Systems of Advice, Support and Response would be more than the proposal for a Cyber Hub. [redacted] confirmed that it would be. [redacted] advised that he and BH will work on the action plan and present it to the Board. They will contact CRU in due course to organise this. ***New action 7 – [redacted] & BH to develop action plan and send to CRU for distribution to the Board for comment. By mid- December***	***[redacted] & BH***
	Learning and Skills DY advised that the draft action plan has strong foundations but reminded the Board that the conversion to measurable actions is a challenge. Once this is done, however, it can be progressed quite swiftly. LMacD advised that Gordon McGuiness wants to include more detail into the existing picture, they also want the plan to reflect the balance between learning and skills. Membership of the steering group will also be worked through in the next couple of weeks. There was discussion on how quickly new issues and development needs arise in this field and [redacted] advised that the new courses being developed have the flexibility to change as things move on and that cyber security issues are moving forward as digital advancement does. [redacted] added that there is a call to industry to take as much responsibility in this matter as the public sector and education does. KN added that we should not forget the role of independent training providers in the plan, particularly around cpd. ***New Action 8:*** [redacted] ***to include independent training providers in the L&S Action Plan. Mid-November.*** **Private Sector**	

	[redacted] talked through the paper she provided, pointing out that this is a short and by no means final paper. She pointed out that the response to cyber threats should be proportionate to the size of an individual organisation and that some idea of what that should be would be very helpful. She also pointed out a gap between ISO and cyber essentials and asked whether this group needs to lead the way in finding something to bridge that. Regarding insurance, [redacted] advised that she will progress this matter with [redacted] next week. **Third Sector** DMcN advised that a start had been made on the action plan and that particular approaches were needed for larger organisations, as well as for medium sized organisations which might not have any expertise in house, but whose Boards may be able to ask the right questions of suppliers. DMcN is keen to reference the action plans for other sectors, rather than create anything bespoke for the 3rd Sector as the issues faced are broadly similar. DMcN advised that the steering group has not yet been identified, but he is looking to bring in people who will provide valuable input and advice. [redacted] agreed that the active defence measures aimed at the public sector as also applicable for SMEs and third sector organisations. He also highlighted, like other sectors, the importance of understanding the cyber risk by accountants and lawyers servicing the Third Sector **Economic Opportunity** [redacted] will provide an update on this at the next Board meeting. ***New Action 9 –*** [redacted] ***to update on the Economic Opportunity action plan at the next meeting.***	[redacted]
8.	**Action summary**	
	New Action 1 – [redacted] ***to arrange working sessions with action plan leads in October or November to discuss interdependencies and timelines.*** ***New Action 2:*** [redacted] ***/***[redacted] ***to engage with Board members' comms leads.*** ***New Action 3 –*** [redacted] ***and*** [redacted] ***to develop comms plans for the strategy, for crisis comms, and for integrated comms for the priority***	***Arranged – 5 Dec*** ***Complete*** ***Ongoing*** [redacted] ***& HA –***

	areas ***New Action 4 –*** [redacted] ***and HA to look into cross party awareness.*** ***New Action 5 – HA will send the paper to the Deputy First Minister (DFM)*** ***New Action 6–*** [redacted] ***will work with HA to arrange a meeting with DFM*** ***New Action 7 –*** [redacted] ***& BH to develop action plan and send to CRU for distribution to the Board.*** ***New Action 8:*** [redacted] ***to include independent training providers in the L&S Action Plan. Mid-November.*** ***New Action 8 –***[redacted] ***to update on the Economic Opportunity action plan at the next meeting.***	***DFM wrote to Parl. Cttee on 8th Nov. Awaiting response.*** ***Complete*** ***Complete – Telephone conference on 1st Nov.*** [redacted] ***/BH*** ***Done*** [redacted]
9.	**DATE OF NEXT MEETING**	
	The Chair thanked everyone for attending. **Next meeting is on 19 December at St Andrew's House, Edinburgh.**	