

Scottish Government
UK Cyber Security Strategy Projects in Scotland

End of year report

PLEASE READ ATTACHED GUIDELINES ON PAGE 5 BEFORE COMPLETING THIS FORM

Details of Grant Recipient

Organisation Name	SICSA (Scottish Informatics and Computer Science Alliance)
Project title	Cyber Nexus: The Scottish Nexus for Cyber Security Research and Innovation
Lead Contact name*	From March 2019: Dr Ishbel Duncan
Contact email address*	Ishbel.duncan@st-andrews.ac.uk
Grant start date	November 2017
Financial year	2019/20

* Please ensure that the current lead contact's details are used here in order that the Scottish Government can update its records accordingly.

Details of Scottish Government Policy Area

Policy Team	Cyber Resilience Unit
Policy Contact Name	Dean Cowper
Contact email address*	Dean.cowper@gov.scot
Contact number	03002442666

To be completed by grant recipient

1. Please detail the progress you have made towards the achievement of your Objectives as set out in your application form.

Objectives	Progress made against each objective. Please also state whether your outcome has been fully/partially/not achieved.
Research and Innovation	<p>Ongoing/ Success:</p> <p>We have clearly established a series of exchanges with research visits to and from experts from across the world. This is ongoing and has already generated knowledge and scholarship. We have growing cohesion between university researchers with commerce and industry specialists through integration events.</p> <ol style="list-style-type: none"> 1. One Innovation Project (11K) has been funded in two parts on a Memory Risk Evaluator for Secure Communication Vulnerabilities (Buchanan at Napier) 2. An early career research visit to the University of Montreal was undertaken in June by Dr. Sid Benabderrahmane from Edinburgh University to exchange work on pattern mining, concept analysis and motifs discovery. 3. Dr Tahaei of Stirling has visited co-researchers in Vancouver for knowledge exchange on developer centred security. 4. Dr Bhowmik of Stirling has attended JPEG standardization meetings in Europe and Australia to work on current standards and to have discussions on the challenges in multimedia such as fake news and forensics. 5. A project on online threat identification to children has been submitted by Dr. Kenwright of Heriot Watt. This project has the potential to be rolled out to online services and agencies. 6. Professor Buchanan is working on an Innovation Hub with Norway, leading on from his research at Napier and he will be submitting a large EU grant proposal. Nexus will help with local funding and with scalability. 7. We have recently had three small security projects submitted for funding on modelling and verification of blockchain (an innovation project), analyzing vulnerabilities on unadministered smart devices for children (research and potential innovation) and lastly working on AI models for security analysis (research).

<p>Education, Skills and Professional Development</p>	<p>Ongoing/ Success: Members of the Cyber Nexus have had or are planning educational events including training and material development for Schools.</p> <ol style="list-style-type: none"> 1. Professor Renaud ran a successful Cyber Security and the Elderly event in April at Abertay. 2. Exchanges and research visits have continued with a research visit from Prof Stephen Flowerday of Rhodes University in South Africa, hosted by the Professor Karen Renaud of Abertay University. The topic was user centred security . 3. Dr. Deepayan Bhowmik of Stirling University is to undertake a visit to Brussels and Sydney for standardisation meetings focussed on blockchain with the JPEG standardisation body on privacy and security activities. 4. Dr Tahaei, from Heriot-Watt, has visited UBC in Vancouver to discuss research and future co-operation on socio-technical aspects of security. 5. A CyberSecurity and Business event was held by Dr Jillian Elder at Perth UHI in April 2019. 6. An event addressing the gender balance in the cyber security industry was held in May 2019 by Dr. Carletta of Edinburgh University. 7. Dr. Jean Carletta is also heading up a workshop on writing a cyber security job description. This is planned for October 2019 in Edinburgh 8. Dr. Jackie Riley of GCU is organising a student cyber convention in Glasgow in October. 9. Two Distinguished Visiting Fellowships have been applied for, but the visitors are unable to visit Scotland until after April 1st. We formally request that the Scottish Government allow these visits to take place as they involve talks at more than one institution, subject to expenses being ring fenced by March 31st. 10. Events are being planned for the Glasgow Science Museum cyber exhibits by Dr. Carletta and Professor Buchanan. 11. Training qualification events are being investigated for January 2020 to be made available for SME staff and university or college staff.
---	---

<p>Leadership and Partnership</p>	<p>Ongoing/ Partial Success:</p> <p>A series of industry focussed events have been identified for university researchers to attend and host a stand advertising CyberNexus events and its potential benefits. Several staff are slated to attend a series of industrial events over the coming months to advertise Nexus events and potential projects directly to SMEs and larger organisations.</p> <p>The Cybernexus.org website is under development by the Investigator to be a one stop shop for industry and to ensure the application process is faster.</p> <p>Our Cyber Integrator , based at Glasgow, has been continually interfacing with industry and government and offering opportunities for collaboration.</p> <p>The Post Doctoral researcher, Dr. Jean Carletta, based at Edinburgh, has been working on multiple events, strategies and future plans. These have included working on gender based projects, helping people write CVs for use and understanding by security professionals. She is to attend a workshop on impact on policy development in October to aid the Nexus outcomes.</p> <p>Other events, such as the serious games for Cyber Security, have partnered academics with games industrialists.</p> <p>The visitor exchanges have garnered interest and attendance from visitors from outwith academia when open talks have been offered. The academic exchanges to EU or overseas institutions are expected to result in research co-operation and academic papers.</p>
-----------------------------------	--

<p>Awareness Raising</p>	<p>Ongoing/ Success:</p> <p>Members of the Cyber Nexus have had or are planning public and professional events including events targeted at partnership and awareness raising with industry.</p> <ol style="list-style-type: none"> 1. Some awareness has been done through the SICSA website but we do not believe that this has been effective as a way to link with industry. Consequently we have started work on the cybernexus.org domain to be launched in October at ScotSoft. 2. External facing events are planned for the Autumn including the Open Rights Group (OrgCon North) public conference. 3. A December early evening industry event is being planned in Edinburgh to draw industry representatives with a leading cyber security speaker. A student poster exhibition will be held alongside this external event to draw attention to the work students are doing and what they can do for industry. 4. Attendance, award support and awareness materials will be distributed at the Scottish Cyber Awards in November 2019. 5. Staff and students attended Glasgow's CyberSec exhibition. 6. There will be a Nexus stand at ScotSoft , Edinburgh, October 3rd 2019 for leaflet distribution and website advertising. 7. Nexus has sponsored the Open Rights Group (Org-Con) North meeting in Edinburgh in October 2019 and will be hosting a stand to raise awareness. 8. An analysis of the state of cyber security training is currently underway. Two Nexus researchers are aiming to roll out training within the next year based on feedback from industry as to training requirements.
<p>Growing Cyber Security resilience in Scotland</p>	<p>Ongoing/Partial Success:</p> <p>Nexus has been represented in several events that have brought together specialists in the area of resilience:</p> <ol style="list-style-type: none"> 1. Dr. Jilian Elder of UWS led an event on cyber security for your business in April 2019. 2. CyberUK was held in Glasgow in April 2019 and six universities were represented at the conference. Areas covered included vulnerability scanning, social media risks, digital forensics and threat information gathering. 3. Cyber Scotland Week included events in Strathclyde, GCU, the College Development Network, Perth UHI, St Andrews and Edinburgh. These events included Cyber Security, Privacy and Trust showcases, a cyber security clinic and a cyber escape room challenge. 4. Napier hosted an introduction to Incident Response at its SOCLAB.

<p>Creating new innovation outcomes and impact in Cyber Security</p>	<p>Ongoing/ Partial Success: SICSA Cyber Nexus has built on the support network built through SICSA and has offered more platforms for joint linkages including research projects, industrial visits and exchanges. We continue to grow awareness within industry and academia in Scotland through public events and have bookings to attend several industrial events before Christmas to advertise possible joint innovation and research projects . There are currently two projects in the early stages of development; 1. a project led by Professor Buchanan at Napier on a risk evaluator for secure communications. The final product will be applicable for roll out through a spin-out company and also have a patent submission. This work is vital for industrial and government defence or cloud based commercial usage. 2. An early stage application from Heriot Watt to work on identifying online threats to children for use by software and game developers is currently under secondary review. This is to ensure that the project outcomes include technical and social outputs for use by software industries, educational fields or policing.</p>
<p>Creating a critical mass of Cyber Security research in Scotland</p>	<p>Ongoing/ Partial Success: The SICSA Cyber Nexus has enabled groups of researchers to exchange knowledge and ideas and plan projects for external funding. We aim to ensure that cyber security is noted as both a technical and a socio-economic impact on society. To this some projects are noted for growth and impact. 1. Professor Renaud has worked on music memory for authentication for elderly and dementia sufferers and ran an experimental workshop at Abertay in the Spring. 2. Professor Buchanan is leading an innovation project on cloud based communications vulnerability assessment. 3. Exchange visits to Australia, Canada and Europe are planned to develop research ties and proposals. We expect to be able to report UK or EU grant submissions and funding at the end of the next session.</p>
<p>Future Projects in discussion or in submission:</p>	<p>A project concerning social support for the hidden community of homeless or dispossessed is expected soon for review (Professors Moncur & Renaud).</p> <p>Support for an Innovation Hub with Norway (Professor Buchanan)</p> <p>Penetration Testing qualification training availability (Dr. Duncan).</p>

2. Describe the key achievements of your project against the agreed objectives [max 250 words]

The role of the Cyber Nexus is to grow more cyber resilience, to aid the economy in this sector and to offer a coherent research presence. To this end we have been baselining the sector and determining a course of action for joint industry and academic workshops and events. We have continued to advertise, interact with and offer events for a variety of attendees including industrial specialists and academics and are planning events for the Winter season to coincide with large conferences attracted to Scotland.

Further work has started on outreach and gender diversity concerns which indicate trigger points for education and outreach. We have outlined some strategic actions for the following six months including a focus on Innovation, raising awareness with the non-academic cyber community and data gathering. We are collating student numbers, courses, theses, projects and potential areas of knowledge and data interchange to enable SMEs to use university knowledge and technical experience, and vice versa. We are growing more connections and events and have a large series of events planned for the coming season to focus on industry SMEs and their cyber security training needs and requirements.

3. Have you experienced any challenges? If so, what actions have been taken in response?

Challenges	Action taken
More named researchers or industrialists are needed to enable knowledge exchange through industry focussed early evening events	We are inviting guest speakers to come and talk. To either breakfast or early evening events. We are currently searching for a well known industrial name to headline our big December event.
More workshops need to be planned in conjunction with external agencies and outwith University schedules.	We continue to work with cyber security organisations (companies and government) to schedule information exchange and training events, but these are often university or industry oriented and not both as we anticipated.
More cohesive engagement by researchers and cyber security specialists	We have regular online meetings every month and are updating our mechanisms for reviewing submissions to ensure a faster turnaround. We have outlined 17 immediate actions to ensure success in cohesion activities and measurable outcomes.

<p>Areas of support not taken up from start of project?</p>	<p>Early Career Support has only had one application and the Innovation Project funding has only recently been applied for. Consequently, the Board has decided to increase the potential amount requested to £5000 and to indicate to industry that this money can be used for innovation, research or resilience training. The Summer School was cancelled in favour of an early December event to attract a well known name in the field for an evening event in Edinburgh, focussed on industry and commerce. The Board decided to plan a student facing event alongside the evening industrial event in December in Edinburgh, date to be arranged. The students will be able to demonstrate and present posters before and after the main evening speaker.</p>
<p>Areas of support taken up from start of project?</p>	<p>All areas are showing some take-up but the most concern surrounds the take up of Innovation and industrial visits. Hence our recent Board meeting to correct our directions and focus more on industry connections (see below). In all, the take-up has been lowest on innovation projects until now and, separately, on early career fellowships. However, events such as workshops, visitor exchanges and fellowships remain popular. Since April 1st we have funded £7,500 directly on events with another £37,800 committed.</p>

Corrective actions	<ol style="list-style-type: none"> 1. We have decided to allow applications for higher amounts, up to £5K in the first instance. 2. To write position papers on strategic areas such as IPv6, digital identity, role of HE and to roadmap HE courses including business and law schools. These quantitative actions of student numbers at BSc, MSc and PhD levels (domestic and non domestics), will baseline where we are in development and also be of use to industry and government. 3. To use deadlined calls open to MSc students for industrial visits. 4. To aim for a general cyber security conference to run with the international Practice and Theory of Public Key Cryptography Cryptography conference (PKC) in May 2020 in Edinburgh. We therefore formally request a no cost detriment past March 31st 2020, to enable us to use that international event as an innovation, research and exposition event for the Scottish cyber community. 5. We will continue to hold open lectures with all hands meetings to discuss what we want and our achievement measures. 6. To build a new website and promotional materials (underway at cybernexus.org) for industry access. We want to enhance the belief that we wish to work together, with and for industry. 7. Allow a faster, two week, turnaround on submissions through online voting or discussion mechanism
Marketing	New website and materials and posters to be ready for October ScotSoft. These will also be used for ORG-con later in the month and the Nexus December event.

4. Please provide a breakdown of actual expenditure to date which this interim report relates, compared to the planned expenditure detailed in your application. Please use broad headings/categories – e.g. travel & subsistence, salaries, etc.

	Actual April to Sept 19	Discrepancy in prior reports to Mar-19	Total Project Spend to Sep-19	Current Future Commitments to Mar 2020
Investigator Time	£3,466.00	–£106,984.00	£20,876.00	£3,754.00
Administration	£8,577.00	£9,758.00	£33,915.00	£8,803.00
Post Doctoral Staff - Edinburgh	£33,165.00	–£8,333.00	£55,183.00	£23,965.00
CyberNexus Integrator - Glasgow	£19,082.00	£31,268.00	£96,067.00	
Travel	£457.00	–£7,440.00	£2,642.00	£150.00
Consumables		–£6,487.00	£1,279.00	
Event Organisation		–£3,470.00	£6,829.00	£1,333.00
Exchanges and Visits	£7,586.00	–£5,771.00	£16,058.00	£6,593.00
PECE				
Research & Innovation				£30,000.00
Total	£72,333.00	–£97,459.00	£232,849.00	£74,598.00

5. Please comment on the breakdown of expenditure in Q4 above, particularly explaining any significant disparities between planned and actual expenditure

It has been discovered that we had submitted for £106K of investigator time prior to March 2019 that has since been added back into the rest of the project. Consequently, we have a discrepancy in our financial reporting that our Finance Advice and Support administrator has adjusted in the orange column above. There is therefore a £25,124 difference between our spending this semester and the discrepancy adjustment (green and orange columns).

We note that there is only £7,500 spent on events over the summer but we have £37,800 committed with the uptake of innovation projects, a series of planned events and £14,000 allocated to small (£3.5K) research and innovation projects recently passed to us from SICSA. The December industry cyber event has not yet been costed as we are currently investigating event spaces and speakers.

As noted in earlier sections we have continued to fund security related visits, exchanges, projects and events. However, the Board were concerned about the slow take up and have decided to increase the potential amount of funding to £5000 and to spend more effort on attracting industry. To this end we have 17 corrective actions, the major seven of which are noted in part 3 above.

Our main events have been industry focussed and now that we have some traction from the events noted in Part 1, we are developing a series of events focussed on training and developing academic – industry ties through studentships, projects and knowledge sharing.

We have more visitors and events that applicants wish to have post April 2020. Consequently, we formally ask if we can ring fence funding for these activities before the March 31 deadline, essentially allowing a no cost detriment to the use of the Cyber Nexus project after March 31st.

6. Was there any underspend? Please provide details of this below.

As shown in the table above, so far £232,849 has been spent on the project to date, with an actual spend of £72,334 in the last six months. However, there was an overestimate of spend prior to March 2019 and the University is aware of a discrepancy of £97,458 as shown above in Part 4 in the orange column. Therefore, there is an overall discrepancy of -£25,124. This has been caused mainly by an overestimate of the time allocation of the previous PI at 30% which was subsequently dropped to 10%.

As far as the outcomes of the grant as concerned the main areas of underspend are in Research and Innovation which has recently started to get traction. We are to focus on this over the next six months and have materials for SMEs and industrial participants at workshops and conferences to spread the message.

Early career and industrial fellowships have had little take up, and the Board are keen to vire this money into take up by SMEs and industry or academic specialists who wish to spend time working in each other's environment on a more variable basis, that may be more suitable to the workplace. Separately, we intend to consider those specialists who are returning to work after illness or leave and require training. We believe security training is a major concern and the Board plans to offer day or short course training to SMEs once two members of the Board have undergone training in appropriate fields, such as penetration testing or vulnerability and risk management.

7. Is your organisation using its grant funding to engage in activity for which there is a market and where income could potentially be derived?

Yes, there is certainly interest and activity in working together to improve research output and an increase in cohesion between academia and industry. However, this has been a slow take-up and interest from industry that perhaps indicates the wariness of the security professional. We are working to offer student internships, white papers, training and investigations which would benefit commercial enterprises.

Funded and to-be-funded projects have already demonstrated groups of people working together, sharing data and writing either academic papers or research and innovation proposals. One of our new actions includes monitoring outputs such as grant proposals, patents or other legal supports for applied technological research. We aim to not only support academic research but to underpin SME and other projects with the necessary legal, ethical or computational framework required to get an innovation or product launched.

A further strand is one of education and training and to this end we are investigating the needs of industry as well as the current state of educational courses in Scotland. We wish to determine if we can offer the Cyber Nexus, or trained staff, for rolling out standards, expertise and qualification support.

8. Please include a short narrative demonstrating the positive impact the grant funding has had [max 250 words]

The funding has continued to allow academics and industrialists to meet and garner ideas, techniques and areas of joint interest. The Cyber Nexus funding has increased research outputs through external travel, project funding, research exchanges and events.

We continue to hold workshops and events to encourage researchers and practitioners to talk and share problems and practice. The Cyber Nexus has allowed work on low level technical research and innovation such as blockchain and signalling as well as high level social aspects such as the use of security by the elderly or dementia sufferers.

We continue to build up our support networks of both educational and technical coal -face practitioners through workshops and discussional, forward thinking meetings. We have also funded gender imbalance, business support and technical risk evaluation projects, to name a few indicators, all of which aid commercial and industrial security development.

Cyber Nexus is allowing and supporting Scottish researchers and practitioners to work together and learn from each other and the growing interest and increase in funding applications for Winter 2019-20 is indicative of us garnering interest from corporate cyber security companies and SMEs.

9. We always value opportunities to illustrate projects/activity. Please briefly detail any activities that could be used as good examples or case studies. [max 500 words]

Case study 1: Professor Renaud of Abertay gave a workshop, funded by Nexus, on security and the elderly that had 80 participants from service providers, civic groups and academia. This successful day has led to potential joint projects with Professor Munro at Dundee on secrecy for the homeless and dispossessed and, separately with Honours/ Masters students on the use of music as an authenticator based on work which Professor Renaud had already initiated.

Case Study 2: Professor Buchanan of Napier is working on MEMDECRYPT, a risk evaluator for secure communication vulnerabilities in Cloud based systems. This work is supported by three companies; Zonefox, Symphonic and Cyan Forensics and will focus on virtualised machines which causes problems with the storage of encryption keys on a permanent or semi-permanent basis. Professor Buchanan has already outlined a potential patent based on a new method for running encryption but the Nexus funding has allowed technical evaluations to be undertaken before patents or papers are published. The project funding also enables discussions with investors once evaluations have been successful.

Case Study 3: Dr Elder of Perth College UHI ran a successful CyberSecurity and business event as part of Cyber Week in April 2019. Speakers included representatives from the Scottish Resilience Centre and Aviva. The event brought together practitioners, school pupils, university students and staff and demonstrated that cyber security applies to many human vectors and business types.

10. Please describe briefly what change your project has made in terms of building Cyber Security? Is there any legacy arising from the result of your project? [max 250 words]

Cyber security researchers and practitioners are working together and bringing their contacts together through events. Cyber Nexus funding has definitely increased the visibility of the research and practice evidenced in Scotland and there is growing industrial and professional interest through previous and planned activities for building these connections into data, work and idea sharing through student internships and research projects. Some projects have already enabled academic research or innovation and others have seeded industrial patents and trials.

The project has been slow to build trust between industry and academic researchers, yet the events and activities noted above indicate that the Nexus project has been extremely useful in creating a viable mechanism for discussion, sharing and enquiry between interested parties.

We intend to continue work on events and growing joint industry – academic projects to demonstrate that Scotland is active in internationally recognised cyber security research, industrial expertise and practice and knowledge sharing amongst the community.

We thank the Scottish Government for allowing Cyber Nexus to act as a seed funder and to grow activities and contacts within the cyber security community.

Signed:	
Date:	September 30 2019

- This report is to be completed by Grant Recipients at the end of each financial year.
- Please complete this form electronically, please feel free to expand tables or text areas as necessary.
- Once complete please send this reporting form by email to dean.cowper@gov.scot

Question	Guidance
Monitoring Objectives	
1	With reference to your objectives, as detailed in your application form, please complete the table. In the first column, list the Objectives and Indicators used to monitor your progress in achieving these. In the second column you should provide an assessment of whether you have achieved the objective in column 1.
2	Please provide a short narrative giving examples of key achievements. This feedback may be used for publicity purposes.
3	Please comment on any challenges you have faced over the reporting period and how you addressed them. Describe the effect or impact that these have had on the achievement of your targets.
Financial Reporting	
4	Please provide a breakdown of actual expenditure in the period to which this report relates, against expenditure planned.
5	Please comment on the breakdown attached in Q4, in particular explaining significant disparities between planned and actual expenditure and giving information on projected expenditure if appropriate.
6	Please comment on any outstanding amount that is left in the budget and provide an explanation for why it has not been spent, bearing in mind that you should have previously alerted the Scottish Government if you were expecting to have an underspend at the end of the financial year. You will need to arrange to speak with Scottish Government on this underspend.
7	If, in the Scottish Ministers' opinion, the Grant or any part of it is state aid and they consider that they are required to recover such sum in order to ensure compliance with their obligations under EU law Scottish Ministers may require immediate repayment of the Grant or any part of it together with interest at such rate and on such basis as may be determined from time to time by the Commission of the European Union.
Further Information	

8	We are interested to hear any stories that illustrate the positive impact the project is having. Please include any further information or comments you feel are important but not covered in this form, that might facilitate the effective monitoring and evaluation of the progress made on you project. Please limit your answer to 250 words.
9	Please use this space to make any further comments you think will illustrate your progress. Like question 3, this is information we could use for publicity purposes or to inform Ministers of progress.
10	Please comment on how your project has contributed towards building cyber security in Scotland. We would be interested to hear of any legacy or sustainability work which will go forward as a result of your completed project.

If you require further guidance on completing this form, please call Dean Cowper on 03002442666