Cyber Eyes Wide Open: Creative Collaboration between Artists, Academics & Cyber Security Practitioners

Abstract. This paper discusses a collaboration between creatives, artists, academics, cyber security professionals and companies to create artworks that increased awareness of cyber security. The aim was to offer creative perspectives and practices into how cyber security might be better understood through creating visualisations, experiences and narratives that could enable communication and insight. 4 cyber security businesses each provided a theme resulting in vibrant collaborations between the companies. 4 academics and 8 artists. 11 projects and 42 pieces of art were developed and exhibited in two exhibitions in the Northeast where over 100 people viewed the works. Evaluation indicated that the artworks had an impact, with people more aware of cyber security. This project has highlighted the opportunities created through collaborations among artists, academics and cyber security practitioners in facilitating the understanding of complex technical issues.

Keywords: Creative Collaboration, User Awareness and Understanding of Cyber Security, Arts and Creativity

1. INTRODUCTION

Creative collaborations have been part of the historical fabric of both academia and creative practices for many decades (Comunian 2016). People have witnessed the application of concepts and ideas from one domain to another completely different setting, resulting in valuable and oftentimes even extraordinary creations. A significant number of scholars and professionals (Walker 2021; Wolff 2018; Osen 2017) have emphasized the positive effects of the creative collaborations not only on the economy but also on our society as a whole. It is easy to see how universities have historically engaged with arts and cultural activities, themselves often patrons or commissioners of art pieces as well as hosts of artists - from poets and writers to architects and musicians – sharing their knowledge through teaching and practice (Comunian 2016). Likewise, arts organisations and industrial sectors have historically benefitted from the knowledge and research developed within academia, from academic articles in arts catalogues to architects benefitting from new materials technologies (Stimuleringsfords 2013; 2015).

A complex new trend which has received increasing attention in academia is interdisciplinary work in creative fields such as arts and computing. Essentially, at this intersection both artists and tech experts have the opportunity to discover new solutions and applications of their work. Where technology has long influenced creative practice, the creative connections from this project consider how art can influence technology. Our brief was to offer routes to understanding of cyber security with the perspective that our cyberworld is vulnerable and breaches of security that have devastating impact on people, organisations and society.

With practitioners from industry, academia and the arts increasing levels of collaboration were considered. Firstly, we saw our groups sharing a space and thinking / creating independently answering the theme with examples of their style of
work. Secondly, we saw contributions that drew upon the various skill sets and ideas to offer shared versions of the tale to be told. Thirdly we saw collaborations that explored new practice and media to develop works that opened new spaces for creativity. Our research question was developed to see whether our project aim to expand understanding of cyber security through art sat alongside our exploration of innovation and creativity. And thus, this paper focuses on the exploratory research question: “do creative collaborations effectively address the specific challenge of raising user awareness of cyber security?”

Section 2 considers creative collaborations and how interdisciplinary approaches can support problem solving. Section 3 provides the cybersecurity context. Section 4 presents the methodology of this study. The make-up of creative collaborations, results and outcomes are described in Section 5 alongside the results of an evaluation exercise undertaken with participants and audiences. Finally, after the discussion of our evaluation exercise in Section 6, the paper concludes in Section 7 with recommendations.

2. CREATIVE COLLABORATIONS

Creative collaborations describe a relationship between two or more persons with a common purpose of creating new objects through certain ideas and shared understanding of something new and a common goal (Tartas & Giglio 2016). New trends in technology and digitization have provided creatives with the opportunity to delve into previously unexplored directions of artistic work (Martinique 2017). With its fast-paced dynamics and constant developments, technology constitutes a widespread area of interest and research for creative professionals (Widewalls Editorial 2017). The creative sector has embraced interdisciplinary practices combining cultural products or processes with new technologies. This has resulted in an increasingly diversified sector, where interactivity, customization and collaboration have emerged as key aspects of this environment (Licheva 2016).

The interdisciplinarity and collaboration between art and technology stands on a solid basis of shared values, such as the passion for innovation and constant improvement. Artists make use of the latest available technologies and materials to express their inner self in the best way possible. Technical practitioners can develop state-of-the-art solutions to make sure that people can use the full potential of today’s interconnected digital world, and to securely bring on the future.

Bronstein (2003) offers a framework for interdisciplinarity consisting of five components: interdependence among the collaborators, newly created professional activities that maximize each collaborator’s expertise, flexibility, collective ownership for the goals and reflection on the process. After establishing why collaboration is seen as necessary in the first place, the purpose and criteria deemed most important for new collaborative projects are summarised in Table 1.

| Purpose of CC | Criteria for selecting new CC |
|---------------|-----------------------------|
| Need for specific expertise | Need for specific expertise |
| Creating a product of high quality | Understanding the different fields |
| Value of feedback and diverse viewpoints | Matching expectations |
|                         | Smooth and clear communication |
|                         | Matching beliefs and goals |
|                         | Ability to get along |

While examining available literature (Gaggioli et al., 2020; Cardenas 2020; & Licheva 2016) and opinions on the topic of creative collaborations and interdisciplinarity, it has become clear that the majority of these studies are mixed methods in nature, typically with significant qualitative elements that enable an in-depth consideration of the issue. This tendency could be explained with the complexity of the topic – the various unique points of view that exist at the intersection of different disciplines may indeed necessitate a predominantly qualitative approach. It has been argued that the ambiguity and changing face of interdisciplinary work in the context of the creative industries also require a more flexible and open-ended approach so that different perspectives could be covered (Licheva 2016).

Qualitative research deals with the participants’ interpretations and understanding of the surrounding world – an approach which usually results in the collection of richer and more in-depth data as compared to quantitative approaches (Ritchie et al., 2013). In addition, qualitative research allows for the uniqueness and nuances of each case or participant to be reflected through the analysis. This characteristic is especially necessary when studying how collaborative projects are conducted considering the diverse nature of the creative companies and stakeholders involved (Sonnenburg 2004). Their distinct work practices would thus be not only difficult to standardize or quantify but by attempting to do so, the complexity and subtlety of certain aspects would easily be lost during the data collection stage.
3. CYBER SECURITY: THE FOCUS OF THE COLLABORATIONS

With data breaches and cyber-attacks on the rise (World Economic Forum's Global Risks Report 2021) and ongoing cyber vulnerabilities and unpreparedness, exacerbated by the tech inequalities within and between societies (SEON’s Global Cyber-Safety Index (2021), cybersecurity is a critical issue. Cyber security breaches are a serious threat to all types of businesses and charities, for example, in the UK 39% of businesses and 26% of charities report having cyber security breaches or attacks in 2021 (Official Statistics 2021). Financial institutions are increasingly experiencing cyber-attacks (Kuepper 2021), as are healthcare systems (Singh 2021) and universities who regularly face ransomware attacks. According to Irwin (2021), organisations face a wider variety of cyber threats than individuals, yet many cyber-attacks are achieved via the individuals in the organisation.

The major cause of many cyber-attacks is phishing which accounted for 32.9% of all reported cybercrime in the US in 2020 (Sharma 2021). Phishing is the fraudulent practice of luring people into revealing personal information, such as passwords, login details and credit card numbers. Through targeting users with a malicious link it is possible to gain access to their account and move laterally within the infrastructure to further disrupt the network and deploy the malware on the end-user devices (Morbin 2020).

The key challenge for organisations is how to tackle the ever-changing threat landscape (Deeney 2020). Security Awareness Training is the best place to start. By training employees with the information required to recognise and react to cyber threats, this mitigates risk and embeds a culture of cyber security awareness. A wide range of approaches have been tried to increase user awareness and understanding of cyber security including workshops (Senthilkumar & Easwaramoorthy 2017), e-Learning platforms (Udroiu 2018), serious games (Hart et al., 2020), theatre plays (Holpouch 2016), and a documentary approach (Kaspersky 2021).

However, here, this paper presents, a somewhat different approach, based on a cohort of creative collaborations. This intervention was part of Creative Fuse North East, a research and innovation project aiming to explore the social, economic and innovative value of the Creative, Digital and IT sectors in the North East of the UK. In June 2021 in collaboration with cyberfest, the annual festival of cyber security in the North East provided by Dynamo, the regional software developer network, creative collaborations - to explore the expression of the concepts of cyber security through the eyes of artists and creatives – began.

4. CREATIVE COLLABORATIONS PROCESS

4.1 Initiate

Cyber security companies were invited to offer ideas for artists and creatives to explore with an aim to aid understanding of their aspect of cyber security. Invitations were sent out to creatives and artists through media channels and regional networks seeking participants to use collaborative, creative practice to explore the understanding of cyber security. Respondents (8 artists and 4 cyber security companies) were invited to an open event, where cyber security companies shared their main issues and challenges and where the creatives including animators, visual artists, poets and ceramicists briefly outlined earlier work and their areas of practice.

4.2 Ideate

Following on from this, the artists and companies identified the ideas that most resonated with them and project groups were formed around themes: 1) People and Technology; 2) Humanity and Security; 3) Animation; and 4) Engaging Young in Cyber Safety. Focusing on the areas of interest of the cyber security companies four teams were formed. Each of the teams included two or more creative practitioners, one or more academics and a member of the research team who facilitated and supported the collaboration. Some creatives engaged in more than one team.

4.3 Innovate

Over the summer, the teams met weekly to discuss, inspire and collaborate developing their artworks. The sessions facilitated engagement between academics, creatives and the Creative Fuse team where shared experiences, inspirations and skills brought new ideas and concepts to reality, allowing innovation in thinking, medium and scale. Our weekly sessions were framed around the participants discussing their progress with their work and preparing to reveal the outputs for their partner businesses at the end of each month. Once a month the whole group met, including all four teams and the companies for reveals and discussions of emerging artworks and where the four themes were heading. The monthly reveal meetings allowed the businesses to respond to the progress of the work and to confirm the content. Through meeting as a whole cohort, the creatives and artists were also encouraged to engage across projects, rather than seeing themselves tied to a single group.

4.4 Implement & Evaluate

Implementation involved exhibitions and evaluations. The exhibition planning attempted to discern whether certain organizational structures in
museums, related policies and procedures resulted in high quality, cost effective and timely exhibitions. Questions of how, when, and by whom visitors would be represented were of paramount importance to the work of making effective exhibitions. A key aspect of the CEWO intervention was to explore the collaborative experience we had aimed to facilitate. To achieve this an evaluator interviewed and discussed the experience with the participants. Comments made were transcribed verbatim and analysed.

*Table 2: Makeup of the CEWO collaborations*

| Collaboration | Theme | Creative | Academic | Outcome |
|---------------|-------|----------|----------|---------|
| People and Technology | SLEEPERS Technology in the Home: Benign Friend or Malevolent Intruder? | painter | musician | The Long Pack Ceramic Alexa as a spy agent in the home settings Alexa: The Friendly Elephant in the Room |
| | | ceramicist | | |
| | | poet | | |
| | | writer | | |
| | | | | |
| Humanity and Security | Exploding Computer Forgotten Password Information Wave Encroaching & winning virus Voice of the Internet | visual artist | visual performance artist | VR 360 Video Clip Chalk Forgotten Password Humanity QR Cyber Rug Hendon Paintings – Great Waves of Information Yorms Blue Humanitas MP3 Sound Track |
| | | digital artist | | |
| | | Poet | | |
| | | Painter | | |
| | | Painter | | |
| Animation | Hidden Messages Layering Information Visibility | visual artist/science explainer | Animator | Hot to Touch Reflective Mirrors Red Filter on the Wall Marigold UV Light Reflective Understanding |
| Engaging Young in Cyber Safety | Fragile World | visual artist | Artificial Intelligence | Glass Globe Glass Mobile Phone Fragile Earth in phases (4X canvas) Photoprints People & Technology |
| | | writer | | |

5. RESULTS AND OUTCOMES

Cyber Eyes Wide Open involved 8 creatives including artists, poets and animators, 4 academics from Computer Science, Art, Design & Media and 4 cyber security companies supported by the Creative Fuse team at Sunderland. 42 artworks were created and exhibited at galleries in Sunderland and Newcastle with over 100 visitors. The works spanned glass, ceramics, paint, photography, voice, performance, 3D, video, poetry and printing.

5.1 Group 1: People & Technology

This project took everyday technologies such as Alexa and looks as to how they can have both positive and negative impacts – benign / malevolence. A series of facsimiles were made with the device magnified and made in clay. This artwork was interactive, with Alexa providing different audio/visual outputs connected to give a randomness in triggers to broadcast. The magnified Alexa was operated via a Raspberry Pi /Arduino etc. with benign, positive and malign outcomes generated. The Alexa outputs and the ‘contents’ were diverse to possibly reflect broad issues including the imbalance of power seen in technology, the underpinning assumptions inherent within algorithms that reinforce behaviours and expectations; the manipulation of data for nefarious purposes; the links between big tech and government; impacts on news and journalism. The poem ‘Alexa the friendly Elephant in the room’ was recited in the room being triggered to play as visitors approached the installations.

*Figure 1: Group 1: People and Technology*

The Long Pack was based on the idea that the SMART speaker enters your home as a help but turns out to be a danger. This is based on a folktales from Northumberland dated 1723. In summary, a wealthy family are spending the winter in London, leaving their country seat on the banks of the North Tyne, in the hands of their servant maid Alice who allows a robber into the home disguised as a ‘long package’. Echoes of allowing technology into the
home disguised as a ‘friend’. This painting was made by combining cobalt pigment (which is an element used in smart speakers), with holy water (which was used for protection) and egg tempera. This was poured and rubbed into a vintage bed sheet, dissected into eight pieces and reformed to make the shape of the long pack.

5.2 Group 2: Humanity and Security

The humanity and security inspiration yielded several individual and group projects, these were subject to the same process of weekly meetings and two reveal sessions where the artists offered their opening work to the companies. The company offered feedback on the work as it came to completion in readiness for the exhibition.

One artist, used as inspiration, Cornelia Parker’s explosion. This has resulted in the development of a concept looking at stills and video of a computer and of it exploding, then converting this into a 360 VR environment with aim being to access the work using VR headsets (HTC Vive/ Oculus) with gaps between images and stills. This piece in the final exhibition was accessed via QR codes, this approach improved accessibility to the work.

Further work in this theme focused on how The Wave of Information is engulfing everyone. The access to so much information is a deluge, and we are submerged, lost beneath a Tsunami of words, sounds and images. The primary 6 ft by 6 ft artwork proposed presents the struggle of the immenseness of information overload. Different informational characteristics are embedded in the waves, positive, negative, benign, dangerous, personal, hidden, etc. Perhaps as boats representing different data types.

![Tsunami, Wave of information](image1)

**Figure 2: Group 2: Humanity and Security**

The computer virus was used as inspiration to create a series of eight digital artworks that explore representations of the first computer worm ‘The Reaper’, invented by Ray Tomlinson in the 1970’s. ‘The Reaper’ is the first example of ‘anti-virus software’. For the work the artist converted personal data files into coding and layered this with the ‘hack’ code used to infiltrate the NHS. This project was seen as a great opportunity to research into the origins of cyber security and allowed the development of new skills in the conversion of JPEGs into Hexagonal coding. The research has been a crucial part of the fusion of art and technology enabling the creation and production of work in both print and video formats. The Yorms were the final output of this group presented as a series of digital prints.

5.3 Group 3: Animation

Initially the project began in a collaborative journey of learning and creativity. Cyber security is a hidden digital ‘thing’ where the work explored materials with properties outside of the visible electromagnetic spectrum and used them to produce hidden images. This idea resulted in artworks focusing on information that is not visible/understandable but then due to a change in perspective the information appears. Tools were provided to ‘decode’ the exhibition.

‘Steal The Shown’ formed a trail of (6) pieces of work, forming a representation of the data that is often stolen through phishing scams and malware. These pieces of information are often hidden in plain sight or given freely.

- Email address – input into any sign-up sheet online
- Password – often used across multiple sites
- Date of Birth – shown on profiles and input into sign-up sheets
- Debit card numbers – input to make purchases
- Bank details – stored on purchase website such as amazon password clues – “cat” can be used to guess passwords

![Reflective Understanding](image2)

**Figure 3: Group 3: Animation**

The artefacts were all displayed in a way that required looking at them with a different perspective using interactive art to complete a puzzle to teach about Phishing scams. The ideas progressed so that the separate pieces formed a hunt and find style trail around the gallery. The title of the combination of works was suggested to be ‘Steal the Show’ or ‘Cyber Art’ so that each one could be linked together with a logo. The title evolved to ‘Steal the Shown’ to be more aligned to the concept where in the cyber world we are willing to show our data even where it becomes a threat to our security.
5.4 Group 4: Engaging Young in Cyber Safety

In this project, the goal was to encourage awareness of cyber safety for university age students / young people with the aim to impact their understanding of cyber security in a ubiquitously technologized world. The installation has several components with a connecting theme to offer an integrated artwork.

Firstly the ‘Perfect World’ was represented by a glass sphere incorporating an aspect of colour that represented the different devices/points of contact with the internet/cyber space. One of the spheres remains whole and perfect, one is smashed and reassembled as a fused glass object such as a phone. The artwork included the sphere on a pedestal. A video piece of spheres being broken and fused back together was made and presented in multiple ways in irregular orders or out of synch.

![Fragile World: Glass Globe](image1)
![Photolith People & Technology](image2)

Figure 4: Group 4: Engaging Young in Cyber Safety

A series of painted canvases of the spheres or abstractions of the spheres, enhanced / augmented with collages of technical objects embedded were made, these showed the decline of the perfect and fragile world. This display was contrasted with a series of real-world photographs showing the emotional relationship between young people and technology.

5.5 Results from the Audience

An exhibition feedback survey was designed as a postcard evaluation to explore the impact of the exhibition on visitors vis-à-vis cyber security. Evaluation postcards were placed in the creative space and the team encouraged visitors to fill in the survey cards. The evaluation postcards included two open ended questions: What was your favourite work, and why? and “Are there any other comments you would like to make about the exhibition itself, or the issues that it covers?”

The survey included one closed ‘killer’ question assessing if the creative collaborations had achieved their aim: “Having seen the exhibition, do you now feel you better understand the issues with cyber security, and your role in it?” with the responses: My eyes are wide open; My eyes are a bit open; My eyes are mostly shut. There were 25 completed feedback postcards.

In response to the closed question, 19/25 selected My eyes are wide open and 06/25 My eyes are a bit open identifying that all of the visitors had further considered cyber security during the exhibition. The 25 feedback postcards indicated that all artworks were appreciated by the visitors, with some visitors unable to choose a favourite: “Like asking for your favourite child. They are all great in their own way”

The most popular of the works was Fragile World. The glass sphere and the video of the glass ball shattering effectively expressed how fragile the cyber world is, and how cyber-attacks can suddenly, powerfully affect our real-world, day-to-day life, with visitors’ comments including: “The glass ball as the whole world, and its shattering due to data and technology.”

The poems and voiceworks broadcast via ceramic Alexas discussing the covert, invasive nature of technology was enjoyed by many, as one visitor noted: “The voice of the poems resonates.”

The Long Pack was found to be very interesting by a number of visitors, including one who commented that it evoked “The concept of spiritual/conceptual protection against virtual intruder.”

Visitors were also entertained by the interactive ‘hidden’ artworks. Comments highlighted that their experience of the exhibition had exposed visitors to the ‘fascinating’ world of cyber security, codebreaking, ciphers and secret communications by presenting devices used to conceal and decode messages.

Overall, comments were very positive, including: “Very interesting talk on cyber security. Thoughtful and well presented. Good standard of work.”

5.6 Results from the Creatives

The creatives involved in the project were interviewed by the evaluator, the interviews were transcribed for analysis. The collected insights from the interviews revealed important interconnected patterns about interdisciplinarity in the context of cyber security but also about the more overarching concepts of engaging in creative collaborations and the communication that goes along with them. More specifically, 5 major and 8 sub themes were identified after completing the coding process:

5.6.1 Positive effects of collaboration

Collaboration in general was heralded as a necessary and enriching approach in achieving greater quality in respondents’ work or in getting
access to expertise which is unavailable in their own skillset.

“The collaboration was instrumental in developing my initial ideas into something more comprehensive and beyond my usual scope. Working with XXX and other artists to develop the ideas was instrumental in this expansion of my work which I found extremely helpful and creative.” (C-V)

“I would consider doing it again and go bigger and better as I have gelled well with a member of another group, and we could work well collaboratively combining our practice.” (C-VII)

“Taking part in this project did help me to move out of a creative slump and helped to give me the impetus to make work. It did add to my portfolio and yes, I did enjoy being involved in this project.” (C-II)

Naturally, the interviewees had different ways of discussing creativity and framing the boundaries of collaborations depending on their own background or experience. Discussion of such differences may be particularly useful in exemplifying the complexities of crossover work. For instance, a few of the respondents pointed out: “The experience did not feel collaborative. My collaborators were not involved in my work.” (C-III)

5.6.2 Eager ness to push the boundaries and experimentation of cyber security

Although cyber security seemed to be the main point, some participants stated: “I would not instigate a project around cyber security as I am an artist and not a technical person.” (C-III)

As is the case with most professions, an artist’s skillset also has its own limits nevertheless, some respondents were keen to push the boundaries and experimentation of cyber security through their artwork: “I would instigate a project myself around cyber security.” (C-VIII)

5.6.3 Diversity powers creative collaborations

The respondents believed in the power of ingenuity to boost cyber security in a technology-driven world.

“Was informed of the project and I was attracted to it because it sounded quite a challenge. Plus, the opportunity to work with such a diverse group of people was of interest to me.” (C-II)

“Overall, this has been a great project, giving me the opportunity to work with diverse group of people and the impetus to produce more work.” (C-VI)

“Collaboration felt OK to me. I enjoyed the whole process in terms of working with others from different disciplines and understand their ideas and concepts.” (C-V)

5.6.4 Creative Collaboration for enhancing knowledge

Due to the highly innovative character of the work, most interviewees maintained that they were continually presented with the possibility of acquiring new knowledge.

“I expanded my knowledge on technology, taking on board the 7 levels of technology.” (C-VIII)

“The work I created was nothing like my current practice.” (C-II)

5.6.5 Main challenges of creative collaboration

The respondents were asked to comment on challenges for their creative collaborations. The following issues were highlighted:

5.6.5.1 Communication

Communication does not always contribute to creative collaboration, but a creative collaboration cannot happen without communication. “The meeting with creative fuse was fantastic we met weekly however the team I was part of managed meetings. All meetings were online.” (C-VI) COVID-19 resulted in a shift towards virtual meetings and due to the increased use of videoconferencing has been challenging for some respondents. “But better communication is needed. Initially we were asked to put forward three ideas to share and outline at the first meeting.” (C-I)

However, some expressed their satisfaction: “The tech company answered emails very well.” (C-V)

“The meetings with creative fuse were fantastic as we met weekly.” (C-VII)

Publicity wasn’t right and this was explicitly identified by several creatives: “Much more advertising needed.” What was key for the artists was that advertising would increase footfall, with the lack of social media around the event failing to provide a “context for visitors to understand and make any decisions whether to visit or not.” “There ought to have been much more publicity in terms of the exhibition in both places such as leaflets, posters, catalogues, press and media.” (C-III)

5.6.5.2 Curation & Gallery Access

Curating the artwork in the first venue seemed to work as a first come first serve caused some issues: “You could have published the call out through curator space, artist network, and Facebook groups such as the North East artist network. it could also be spread via the council culture teams. This may have gotten you additional responses.” (C-III)

“This was the first time I felt that the curation of the show as a whole was very ‘degree show’ like.” (C-I)

Some respondents commented on exhibition venues. “More accessible venues would be better”. (C-III)

“Some external signage would definitely help. I arrived but wasn’t sure where to go, or even the event was on.” (C-V)
Few respondents expressed their concerns about invigilating gallery spaces: “I invigilated on two occasions. On one occasion I was completely alone, and I did not feel safe.” (C-VIII)

5.6.5.3 Time & Money
Some respondents were not happy with time given to them to produce their artefacts: “The overall project timescale was quite challenging….working under time pressure was hard.” (C-II)

For some time was not an issue: “Time was OK for me. The pace was good for doing multiple projects.” (C-IV)

“The time allowed was fine.” (C-VIII)

A few artists highlighted the issue of late payments: “Still waiting for payment. I had to buy and pay for all the products myself. So, I am currently in debt.” (C-III)

“I still require the final payment and the materials payment to be processed and paid.” (C-V)

5.7 Results from the Creatives

This section has described the aspects of the project highlighting the works created by the artists and the groups in response to the practitioner brief. The evaluation process for the project was explored highlighting the findings from both the audiences and artists. Our findings as evidenced above are discussed below, against the concepts of cyber security awareness and creative innovation.

6. DISCUSSION

Cyber security is a matter of major importance for companies and authorities globally. Historically, the subject was exclusively addressed by a narrow circle of specialists. The challenge now is to find the way to open understanding of such threats as widely as possible. The lack of user awareness and knowledge of cyber security has been considered a contributing factor to the increase in cyber attacks and cyber threats (operations (Jean-Pierre 2021; Maassen 2018; Udroi 2018; and Skarga-Bandurova et al., 2016). According to Senthilkumar & Easwaramoorthy (2017) found that awareness can be developed by increasing the exposure of people to issues of cyber security through cross-disciplinary creative collaborations.

Cornell (2019) suggested that as malevolent actors are constantly working together, sharing tools and techniques for penetrating security systems, that the only chance we have of keeping up is to work together as well. Just as countries align against common enemies, we must adopt a similar posture or will likely fall further behind. Personal and sensitive data such as credit card details, text messages and photos now clutter our digital world. As a result, it has become more difficult to effectively take care of such vast amounts of information – making its protection a skilful art. Online privacy, and the impact that data breaches can have on a person or an organization, are critical risks to everyone in this connected age. Therefore, keeping our personal data and online interactions secure is fundamental to ensuring technology continues to play a positive and essential role in our lives (Kaspersky 2021).

Ford (2021) argues that there is no single tool or security concept that will have a greater impact on the overall cyber landscape than that of collaboration. Creative collaborations can also be understood as an innovative method of alternative knowledge production, for example foregrounding collective, participatory, or embodied forms of knowledge (Johnstone 2021). In view of this, this Cyber Eyes collaboration among the artists, academics and tech-professionals stands on a solid basis of shared values, such as a passion for innovation and constant improvement. The artists made use of the latest technologies and materials to express their inner selves in the best way possible. By jointly presenting the art piece the cybersecurity companies, academics and the renowned artists aimed to raise awareness about online privacy, which goes far beyond safeguarding data, to protecting people’s digital identities.

Participants of this study engaged for different reasons. For cyber security companies their goal is to collaborate with creative practitioners to explore perspectives, visions and understanding of cyber security; and to have an artwork leaving them with a new creative way to represent their business and values. For artists and creatives, the rationale to engage was to find exciting ways to innovatively visualise, perform and represent cyber security and to gain exposure and possibly new markets for them and their works. For the Creative Fuse researchers, the goal was to explore how to facilitate this type of innovation and the value that such collaborative approaches might bring. The attraction to create this project was based on the idea of bringing two very different worlds together into the Creative Fuse community. These creative collaboration with artists, academics and cyber security professionals has resulted in a natural synergy in which parties with different skill sets worked together in balance to create a unique project.

This work explored a number of practical considerations for artist-academic-industry collaborations, with a particular focus on projects relating to cyber security awareness. Within the digital humanities – a field defined by its enthusiasm for collaboration, interdisciplinarity and dialogue – artists are often engaged as part of multi-disciplinary teams, or to work with individual academics on specific projects. Collaborations between
researchers and creative practitioners are generally perceived as highly desirable, with potential benefits for both sides: they are often recognised as a way for academics to bring their research to a wider public, and for artists to access expert knowledge that can be used as raw material for their own work. This project took this collaboration a stage further by engaging with practitioners and exposing them to the creative process.

We believe the key benefits of our approach are that it considers the grand challenges of the future that very little work has previously covered. It is an art-based reasoning approach which allows for the benefit of making use of different levels of abstractions to raise people awareness on different types of cyber-attacks with potentially socio-technical harm. It is a starting point for research into cyber security, intended to provoke discussions and awareness. The key limitations of our approach are that it is largely conceptual and generic presently as it stands, with little empirical or experimental evidence to support the assertion that our approach will be successful in other domains. This also opens up the possibility of each research project involving artists, academics and tech-professionals using the approach differently, making it challenging to ensure that projects apply as intended.

7. CONCLUSION

This paper outlines how collaborations between artists, academics and IT professionals are initiated, the processes that are involved, and the outputs that might be expected. It also highlights the symbiosis between Higher Education and the Creative Economy (CE), but also the recent pressure and policy interventions that have placed creative collaborations high on the agenda of both academics and practitioners. Some valuable lessons were learnt regarding the relationship between universities and practitioners, around a lack of fluidity of processes, timeliness in making payments and communicating in a commercially astute way. This knowledge will inform future interventions for this project at least. By conducting this study, we were able to establish how the level of user awareness and knowledge of cyber security could be impacted by targeted awareness training. Moreover, the results of this study contribute to bridging the gap between the practice and the theory. With this information, users are empowered with knowledge that can address the factors affecting cyber security, incorporate cyber security in strategic planning, and implement creative collaborations, involving academics, creatives and cyber security professionals, with the objective of achieving a resilient cyber security environment.

REFERENCES

Bronstein, L. R. (2003). A model for interdisciplinary collaboration. Social Work, 48(3), 297-306. doi:10.1093/sw/48.3.297.

Cardenas, E and Rodegher, S.L. (2020). Art-Science Collaborative Competencies: A Mixed-Methods Pilot Study for Improving Problem Solving for Sustainability Challenges. Sustainability 12, no. 20: 8634. https://doi.org/10.3390/su12208634.

Comunian R. (2016), ‘Creative Collaborations: the role of networks, power and policy’, in Shiach, Morag, and Tarek Virani, eds. Cultural Policy, Innovation and the Creative Economy: Creative Collaborations in Arts and Humanities Research. Springer, pp.231-244.

Deeney, N. (2020). Why is Security Awareness Training Important? MetaBlog. Retrieved on 28 May 2022 from https://www.metacompliance.com/blog/why-is-security-awareness-training-important/

Ford, K. (2021). The Future of Cybersecurity is Collaboration. CyberGRX. Retrieved on 28 May 2022 from https://www.cybergrx.com/resources/research-and-insights/blog/the-future-of-cybersecurity-is-collaboration

Gaggioli, A., Mazzoni, E., Benvenuti, M., Galimberti, C., Bova, A., Brivio, E., Cipresso, P., Riva, G & Chirico, A. (2020) Networked Flow in Creative Collaboration: A Mixed Method Study, Creativity Research Journal, 32:1, 41-54, DOI: 10.1080/10400419.2020.1712160.

Hart, S., Margheri, A., Paci, F., and Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education, Computers & Security, Volume 95, 101827, ISSN 0167-4048,<https://doi.org/10.1016/j.cose.2020.101827>

Holpuch, A. (2016). Privacy: Edward Snowden and Daniel Radcliffe co-star in off-Broadway play. The Guardian. Available at: <https://www.theguardian.com/stage/2016/jul/01/privacy-edward-snowden-daniel-radcliffe-off-broadway-play>.

Irwin, L. (May 27, 2021). What is cyber security awareness and why is it important? it Governance. Available at: <https://www.itgovernance.co.uk/blog/what-is-cyber-security-awareness-and-why-is-it-important>

Johnstone, F. (2021). Collaborations between artists and academics. Working Knowledge/Hearing the Voice, Durham University, UK. Retrieved on 28 May 2022 from: https://hearingthevoice.org/wp-content/uploads/2021/01/Johnstone_Collaborations_Academics_Artists.pdf
Kaspersky (Jan 28, 2021). Security is an art: Kaspersky teams up with contemporary artist Felipe Pantone to raise awareness on Data Privacy Day. Globenewswire. Available at: <https://www.globenewswire.com/news-release/2021/01/28/2165892/0/en/Security-is-an-art-Kaspersky-teams-up-with-contemporary-artist-Felipe-Pantone-to-raise-awareness-on-Data-Privacy-Day.html>

Kuepper (February 24, 2022). Cyberattacks and the Risk of Bank Failures. Investopedia. Available at: <https://www.investopedia.com/articles/personal-finance/012117/cyber-attacks-and-bank-failures-risks-you-should-know.asp>

Licheva, Z. (2016). Interdisciplinary Collaboration in the Creative Industries. Master's Thesis. Erasmus University Rotterdam.

Maassen, M. A. (2018). Opportunities and risks of the agile software development management in the IT field. Case study: IT companies between 2009-2018. Review of International Comparative Management / Revista de Management Comparat International, 19(3), 234–243. <https://doi.org/10.24818/rmci.2018.3.234>

Martinique, E. (2017). Celebrating a Future of Diverse and Changeable Identities - In Conversation with Filip Custic. WIDEWALLS. Available at: <https://www.widewalls.ch/magazine/the-serious-relationship-of-art-and-technology>

Morbin, T. (Oct 15, 2020). Why are educational establishments so vulnerable to cyber-attack? Teiss. Available at: <https://www.teiss.co.uk/news/why-are-educational-establishments-so-vulnerable-to-cyber-attack-8509>

Official Statistics (Mar 24, 2021). Cyber Security Breaches Survey 2021. GOV.UK. Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021#fn:1>

Osen, M. (2017). The Importance and Benefits of Collaborations in Creative Business. Available at: <https://marketing.com.au/the-importance-and-benefits-of-collaborations-in-creative-business/>

Ritchie, J., Lewis, J., Nicholls, C.M. and Ormston, R., Eds. (2013) Qualitative Research Practice: A Guide for Social Science Students and Researchers. Sage, Thousand Oaks, CA.

Senthil Kumar, K. & Easwaramoorthy, S. (2017). A Survey on cybersecurity awareness among college students in Tamil Nadu. IOP conference series. Materials Science & Engineering, 263(4), 1. https://doi.org/10.1088/1757-899x/263/4/042043

Singh, H. (Dec 29, 2021). Healthcare Cybersecurity: Threats and Mitigation. Infosecurity. Available at: <https://www.infosecurity-magazine.com/blogs/healthcare-cybersecurity-threats/>

Sharma, S. (12 November 2021). Global Cyber-Safety Index. Available at: <https://www.csoonline.com/article/3640710/which-countries-are-most-and-least-at-risk-for-cybercrime.html>

Skarga-Bandurova, I., Ryazantsev, A., and Kyrushatova, K. (2016). An experience report on education and training programme in cybersecurity of critical infrastructures. Information & Security, 35(2), 123–132. https://doi.org/10.11610/isij.3506.

Sonnenburg, S. (2004) Creativity in Communication: A Theoretical Framework for Collaborative Product Creation. Creativity and Innovation Management, 13, 254-262. https://doi.org/10.1111/j.0963-1690.2004.00314.x

Stimuleringsfonds. (2013). Crossover works #1. Innovating with the creative industry. Stimuleringsfonds Creatieve Industrie. Available at: <http://stimuleringsfonds.nl/en/latest/news/crossover_works_1/592/>

Stimuleringsfonds. (2015). Crossover works #4. Healthcare innovations with the creative industries. Stimuleringsfonds Creatieve Industrie. Available at: http://stimuleringsfonds.nl/nl/het_fonds/activiteiten/publicaties/crossover_works_4/

Tartas, V., & Giglio, M. (2016). Collaborative Design in School: Conflicts, Contradictions, Agreements, and Disagreements to Learn. In E. Railean, G. Walker, A. Elçi, & L. Jackson (Ed.), Handbook of Research on Applied Learning Theory and Design in Modern Education (pp. 420-438). IGI Global. https://doi.org/10.4018/978-1-4666-9634-1.ch020

The Global Risks Report (Jan 19, 2021). 16th Edition. World Economic Forum. Available at: <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf>

Udroiu, A. M. (2018). Implementing the cybersecurity awareness program using e-Learning platform. ELearning & Software for Education, 4(43), 101–104.

Walker, D. (2021). Fuelling the creative economy through creative collaboration. Creative Culture & Capital. Available at: <https://www.creativityculturecapital.org/blog/2021/09/13/%E2%80%9B%E2%80%9Bfuelling-the-creative-economy-through-creative-collaboration/>

Widewalls Editorial (July 25, 2017). The Serious Relationship of Art and Technology. WIDEWALLS. Available at: <https://www.widewalls.ch/magazine/the-serious-relationship-of-art-and-technology>

Wolff, B. (2018). The Future Of Work Is Creative Collaboration. Forbes. Available at: <https://www.forbes.com/sites/benjaminwolff/2018/08/14/the-future-of-work-is-creative-collaboration/>