Research Paper

Cybersecurity in UK Universities: mapping (or managing) threat intelligence sharing within the higher education sector

Anna Piazza[1], Srinidhi Vasudevan[1] and Madeline Carr [ID][2],*

[1]School of Business, Operations and Strategy, University of Greenwich , Old Royal Naval College Park Row Greenwich SE10 9LS, London and [2]Department of Computer Science, University College London, Gower Street WC1E 6BT, London

*Correspondence address: Gower Street London WC1E 6BT. E-mail: m.carr@ucl.ac.uk

Abstract

Higher education has recently been identified as a sector of concern by the UK National Cyber Security Centre (NCSC). In 2021, the NCSC reported that universities and higher education institutions (HEI) had been exponentially targeted by cyber-criminals. Existing challenges were amplified or highlighted over the course of the global pandemic when universities struggled to continue to function through hybrid and remote teaching provision that relied heavily on their digital estate and services. Despite the value of the sector and the vulnerabilities within it, higher education has received relatively little attention from the cybersecurity research community. Over 2 years, we carried out numerous interventions and engagements with the UK higher education sector. Through interviews with cybersecurity practitioners working in the sector as well as roundtables, and questionnaires, we conducted a qualitative and quantitative analysis of threat intelligence sharing, which we use as a proxy for measuring and analysing collaboration. In a unique approach to studying collaboration in cybersecurity, we utilized social network analysis. This paper presents the study and our findings about the state of cybersecurity in UK universities. It also presents some recommendations for future steps that we argue will be necessary to equip the higher education sector to continue to support UK national interests going forward. Key findings include the positive inclination of those working in university cybersecurity to collaborate as well as the factors that impede that collaboration. These include management and insurance constraints, concerns about individual and institutional reputational damage, a lack of trusted relationships, and the lack of effective mechanisms or channels for sectoral collaboration. In terms of the network itself, we found that it is highly fragmented with a very small number of the possible connections active, none of the organizations we might expect to facilitate collaboration in the network are playing a significant role, and some universities are currently acting as key information bridges. For these reasons, any changes that might be led by sectoral bodies such as Jisc, UCISA or government bodies such as NCSC, would need to go through these information brokers.

Key words: cybersecurity, higher education, university, social network analysis, collaboration, threat intelligence sharing

Introduction

A strong higher education (HE) sector is one of the brand marks of the UK (See the 'Great Britain' campaign for examples of how UK higher education is perceived as part of the national identity. 'Great Minds are always open to new ideas'. https://www.greatcampaign.com/post/seeing-things-different ly-capturing-the-spirit-of-a-nation.). It provides a research base for innovation by attracting the best and brightest academics and stu-

dents from around the world. For those coming from (and returning) abroad, the HE sector helps to export UK values and norms. The overall contribution to the UK economy by universities in England was estimated at £95b in 2021 (The HE sector is comprised of universities, further education colleges, higher education colleges, government bodies such as Department for Education (DfE), public sector bodies including Office for Students (OfS), funding councils and representative bodies including Universities UK (UUK), Universities Scotland, Universities Wales, Association of Colleges, and GuildHE. As of 2017, there were 163 higher education institutions (HEI), 241 further education colleges and 732 alternative providers (HESA list of providers 2022 accessed from https://www.hesa.ac.uk/support/providers/all-hesa-providers). In our study, we focus on universities and do not include further education colleges or alternative providers.). Universities contributed £52.9 bn to the UK GDP, accounting for 2.9% of all economic activity for the year 2021 (Ibid). The sector represents over 2.38 million students, and 815 000 jobs in England alone (ibid).

In this context, HE has unfortunately been identified as a sector of concern by the UK NCSC [1]. In 2021, the NCSC reported that universities and HEI had been exponentially targeted by cybercriminals [1]. Existing challenges were amplified or highlighted over the course of the global pandemic when universities struggled to continue to function through hybrid and remote teaching provision that relied heavily on their digital estate and services. Despite the value of the sector and the vulnerabilities within it, HE has received relatively little attention from the cybersecurity research community.

A recent report [2] reviewed the risk reports for 22 HEIs for insights into how they viewed the risk likelihood and impact of cybersecurity. Cybersecurity and information governance is seen as one of the top risks reported by these organizations, featuring on risk registers 50% of the time. As with other sectors, collaboration is understood to be significant for the HE sector [3, 4] but to date, there has been little in the way of sector wide collaboration. In research into other sector specific cybersecurity, the extent to which collaboration and information sharing has been effectively implemented within the ecosystem has been identified as an important factor in mitigating against cyber risk. There have been several studies that have investigated similar ecosystems to better understand the contextual human and organizational factors that affect cybersecurity. These include leadership [5], organizational structure and dynamics [6], group cohesion [7], diverse membership and affiliation [8] and collaboration [9].

Given the significance of the UK HE sector, the NCSC concerns about it, and the established view that information sharing is key to successfully dealing with cybersecurity risk, understanding and explaining the factors that encourage and impede collaboration among HEIs was the motivation for this work. We approached this through an empirical study of the collaborative relationships and the network structure of the sector. Our starting point is two well-established observations: first, that collaboration allows individuals within organizations to access information and knowledge with the aim of improving ecosystem cybersecurity and resilience [10]; and second, that collaborative relationships are established through cyber threat intelligence sharing which supports peer learning [11].

Building on these observations, our work extends prior research on cyber threat intelligence sharing in two ways. First, we use social network analysis (SNA) to investigate how collaborative relationships are established and function within the HE sector. More specifically, we identify the characteristics of the collaboration network as well as the most central institutions to better understand the networking behaviour among organizations. Our study found that the

collaboration network in UK HE has significant scope for improvement and most of the recommendations for action lie with university management and with the organizations established to support university IT and cybersecurity practitioners.

Our second contribution is that we determine benefits and obstacles to collaboration behaviour in the context of cybersecurity threats using qualitative data. Prior research has shown the importance of examining the different factors that encourage collaboration and influence the decision-making process of individuals and organizations regarding sharing cyber threat information [5, 12]. We found that most individuals who engaged in the study were strongly inclined to share information but that institutional and sectoral factors too often prevent that.

The remainder of the paper is organized as follows. We briefly outline our methodology including how we use SNA, our data collection methods, and our conceptual framework. Following this, we provide some insights into the UK HE sector including some of the factors that make this sector uniquely challenging, and we outline the key organizations that populate the ecosystem. This is followed by two substantive sections. The first contains the results and discussion of our SNA of the sector. The second outlines the key factors that our study identified as impediments to better collaboration within this sector. The final section concludes the paper providing recommendations for the HE sector and those who support it.

The findings of this study are specific to the UK HE sector but perhaps more significantly, the methodology we have designed and employed (SNA) could be replicated in other sectors to map those ecosystems and to better understand collaborative relationships. Additionally, while universities are similar in many ways to other similar-sized organizations and face many common cybersecurity challenges, there are certainly ways in which this sector is unique, and we argue that understanding those unique qualities will be central to improving cybersecurity in this critical sector.

Methodology

The main goal of this research was to map and analyse the collaboration network of organizations within the UK HE ecosystem as well as to identify the factors that facilitate or impede collaboration within that network. To do this, we adopted a mixed methodology based on interviews with senior leaders and individuals responsible for organizational cyber resilience. We triangulated this with findings from quantitative data. This approach has been successfully used to map collaboration networks in other settings such as healthcare [13].

Prior research has emphasized the importance of using SNA to map collaboration partners and to quantify organizational behaviour [14] because it provides a set of tools and theories to understand the relationships amongst relevant individuals and organizations [15].

Data collection methods

The empirical part of this study relies on primary data sources. There were two stages to collect our primary data. In the first stage, we conducted 17 semi-structured interviews with Chief Information Security Officers (CISOs) from different UK universities. Where there was no CISO, we interviewed the person who was responsible for organizational resilience or directly involved in designing the cyber strategy. Compared to other similar-sized organizations, relatively few UK universities had a CISO role in 2021 (although this is becoming more common). The purpose of these interviews was to gain background insights and to help develop and refine the questions for a wider questionnaire. We asked the participants questions about the

specific cyber challenges pertaining to the HE sector, their perceptions of collaboration within the sector, any barriers to collaboration that they encountered; and their recommendations for changes that might improve this.

With this information, we analysed and prepared the materials for designing the questionnaire. The questionnaire focused on three main themes: (1) collaboration networks; (2) perceptions about collaboration including the factors that facilitate or impede collaboration in the sector; and (3) demographic information at individual and organizational levels. Specifically, in the first part, we measured collaboration by asking 'with which organizations within the HE sector have you collaborated most frequently in the past year?'. Participants were asked to select those organizations from a list provided and they were also asked to add other organizations that were not included in the list. We used this network question to map the interorganizational collaboration relations among universities and other organizations, to measure network characteristics, and to calculate the centrality measures (which organization/s were closest to the centre of the network).

In the second theme of the questionnaire, we asked about the respondents' collaboration experiences. In line with existing literature [16, 17], we used a Likert-type scale to ask respondents to indicate how much they agree or disagree with statements such as (i) collaboration helps to develop solutions for cyber security problems; (ii) collaboration helps to develop a sense of community; and (iii) collaboration encourages mutual learning. Perceptions of obstacles to collaboration were also measured through six questions.

Finally, in the third theme of the questionnaire, we asked for organizational information including the location of the university, their cybersecurity budget allocation, and individual information such as the respondent's role, tenure and gender. We presented the questionnaire synchronously to 113 participants during an online roundtable hosted by UCISA on 17th of August 2021. The respondents were all responsible for cybersecurity for their university. The research team was available throughout this phase of the data collection process to address any questions or concerns from the respondents. The response rate was 82% with the vast majority of them being male (85%). In terms of their role descriptors, many of them were Director of IT/IS Security (30%), 24% were Cyber Security/Assurance/IT/Networks Manager and a further 19% were Head of Networks/IT. Interestingly, only 6% of them carried the title of CISO (Please note: In our paper, we refer to our participants as CISOs although this does not reflect their title. All interviewees were responsible for IT/Library Services/Security within their organization.). Their tenure ranged from less than 1 year (6%) to more than 10 years (40%) of employment with 22% having worked in their role for 1–3 years. Most of the universities represented were located in England (80%) with 2% in Wales, 17% in Scotland and 1% in Northern Ireland (as shown in Table 1).

Due to the pandemic, the interviews, the roundtable and the questionnaire were conducted online using Microsoft Teams. We conducted the interviews and the roundtable with audio and video to capture non-verbal behaviour including gestures and body movements, that support social exchange and interaction [18] and to obtain a sequential observation scheme recording the real-time of interaction. The interviews were transcribed and analysed using NVivo 12, which allowed us to identify common themes and issues. In both stages, that participation was voluntary, and the data were kept in strict confidence and in adherence with the Data Protection Act. The ethical form was approved by the UCL Ethics Committee (19297.001).

Table 1. Participant characteristics

Dimension	Category	%
Gender	Male	85
	Female	15
Role	CISO	6
	CIO	6
	CTO	1
	Director-IT/IS/Security	30
	Head of Networks/IT/GRC/ ICT/Security/IST	20
	Head of Operations	2
	Head of Digital Architecture	1
	Cyber Security/Assurance/IT/ Networks Manager or associate level staff with no managerial responsibilities	24
	IT Infrastructure Project Manager	1
	Information Assurance Officer	1
	IT Operations Manager	1
	Information Security Manager	5
	Infrastructure Manager	2
Tenure	<1 year	6
	1–3 years	23
	3–5 years	14
	5–8 years	10
	8–10 years	7
	>10 years	40
Organization location	England	80
	Wales	2
	Scotland	17
	Northern Ireland	1

The table below provides information on the questionnaire respondents.

Social network analytic framework

Understanding how social interaction influences behaviour is critical for devising and implementing effective interventions [19]. SNA refers to a set of theories and techniques that helps researchers to understand how social actors—organizations, in this case—interact with others [20]. A network is defined as a set of nodes (e.g. organizations) and a corresponding set of relations (e.g. cyber threat intelligence sharing), which is represented as a line connecting nodes [15]. In our study, we treat the sharing of cyber threat information as the observable counterpart of the propensity for organizations to collaborate via the creation of network ties. Existing research has shown that cyber threat sharing relations cannot persist without mutual communication, knowledge exchange, and sharing best practises between partners [21 p.11]. Cyber threat information sharing typically occurs when one (sender) organization that has been attacked shares (sensitive) intelligence to others (receiver) outlining the details of the attack.

We use these node and network-level measures to understand the collaborative patterns in the cybersecurity ecosystem in the UK HE sector. Node-level measures include 'centrality', which refers to the most central organizations in the network. This is determined by the number of incoming ('in-degree') and outgoing ('out-degree') relations [22]. The 'betweenness centrality' refers to the number of times an organization is on the shortest path between any two nodes in the network. This indicates that this organization acts as an 'information broker' or 'bridge' in the network [23]. Finally, the 'Hypertext Induced Topic Search' (HITS) algorithm [24] enables us to recognize

the role that each node plays in providing information ('authority') or its role in linking other nodes to the information source ('hub'). We also use network-level measures such as 'density', 'reciprocity' and 'network diameter'—all of which characterize the overall structure of the network. Density in a network shows the proportion of *actual* relations over *potential* relations [15], which provides insight into the overall connectivity of the network. Reciprocity shows the number of times a tie is reciprocated—for instance, in the case of this network, not all information *receiving* nodes also *send out* threat intelligence [15]. We use an SNA software tool called UCINET 6 to calculate the individual and network measures described above and Gephi (There are different network software that helps researchers to map and visualize the sociogramme. In this work, we use Gephi, and in particular, a feature called No-Overlap to ensure that all nodes are clearly visible in the interorganizational collaboration network).

This combination of interviews, questionnaire data and SNA allowed us to gather significant and novel insights into how the UK HE sector collaborates on cybersecurity threat intelligence sharing as well as which factors impede further collaboration. It also allowed us to draw out recommendations for how this could be improved going forward. The next section of the paper provides a list the relevant organizations that support or interact with universities on cybersecurity. They are all part of the network in question and are discussed below in the SNA.

Overview of sectoral actors

In many ways, HEIs are similar to other large organizations and face common cyber security risks. One of our interview respondents who had only recently moved to the HE sector observed that 'you have the same risk in HE as you have in other firms… you are compromised, your information is stolen, released, and you are on the front page of the Daily Mail … underneath that is the business continuity risk that, through ransomware or something else, your business is stopped… I think that is a pretty common pattern in an enterprise or in a business' (Int1).

However, there are also some distinct features of HEIs that make them particularly interesting and arguably, uniquely challenging, from a cybersecurity perspective. Some of these include the extent to which universities are dealing with high turnover in an increasingly casualized workforce and onboarding thousands of new students every year in a constricted period of time. There are also challenges pertaining to protection of high value intellectual property, an institutional culture that does not prioritize non-critical rule following, governance and committee structures that can preclude or discourage information sharing, and budgetary constraints.

While people working in HEIs may be as willing to share threat intelligence information as those in any other sector, this can happen through bilateral or small group relationships (less sustainable and impactful on the ecosystem) or it can happen through organizing bodies. There are a range of support organizations in both the public and private sectors that carry out specific functions for the HE sector or provide specialized cybersecurity support. Within these, there are several organizations that are specifically focussed on providing information technology or cyber security support. One or some of these should fulfil that role of an information sharing platform though our research did not find any of them to be functioning as well as required.

NCSC: The National Cyber Security Centre (NCSC) is a government agency and part of the GCHQ (Government Communications Headquarters). It is responsible for monitoring cyber incidents, pro-

viding timely warnings, disseminating cyber-related information and providing technical support to organizations and the wider public in the UK. The NCSC acts as a single point of contact and aims to provide practical guidance on responding to cyber security incidents [25].

CPNI: Centre for Protection of National Infrastructure (CPNI) is a government agency that aims to protect and provide security advice for the national infrastructure of the UK. As part of its remit, the CPNI runs the Trusted Research campaign that provides guidance on improving and protecting sensitive research data, intellectual property and personal information without unduly stifling innovation through international collaborations [26].

UCISA: The Universities and Colleges Information Systems Association (UCISA) is a member-led, not-for-profit professional body that provides resources about technology leadership, digital transformation, protection of digital technologies and data, as well as cyber security best practices. It acts as a channel for dissemination of cyber threats and uses its network of members to relay information that it receives on cyber threat intelligence [27].

CiSP: The Cyber Security Information Sharing Platform (CiSP) is a joint partnership between the government and industry, run by the NCSC. It helps organizations share timely threat intelligence in a confidential and secure manner. Although not specific to the HE sector, the CiSP platform is utilized by professionals and practitioners within HE who are responsible for cyber security in their organization [25].

Jisc: The Joint Information Systems Committee is a subscription based, not-for-profit body that provides UK research and education institutions with digital solutions and support. This includes procurement frameworks, negotiated sector-wide fees for products and services and access to the more secure Janet network. Jisc also offers advice, paid consultancy and training services to the sector [3].

HEIDS: The Higher Education Information Directors Scotland is non-profit professional body that provides resources about digital transformation, technology leadership, best practices in cyber security and protection of digital technologies. It is part of UCISA and operates within UCISA's charitable objectives. Within UCISA, it plays an important role for disseminating and receiving cyber threat information within the Scotland Higher Education sector [28].

Private sector organizations: There are many private sector organizations that provide IT/security, data management, cloud-based services and IT infrastructure on a fee for service basis to the HE sector. Managed Service Providers (MSPs) are part of this stakeholder group and are becoming more attractive for HE institutions given that, like most large, publicly funded organizations, most of these institutions lack the expertise and adequate budgets to keep pace with the fast-moving cybersecurity threat landscape [29]. Private threat intelligence sharing companies are also increasingly used by HE institutions. Specifically, Microsoft has a significant role to play due to the reliance of the UK HE sector on their products.

SNA

The interorganizational collaboration we recorded includes 177 organizations from the UK HE sector. Through our survey instrument provided in Appendix 1, we constructed a one-mode network (A one-mode network is a network that has one set of nodes that are similar [15]). In our case, our network nodes are organizations that are connected through the threat intelligence sharing relationship, resulting in 366 ties. Organizations include universi-
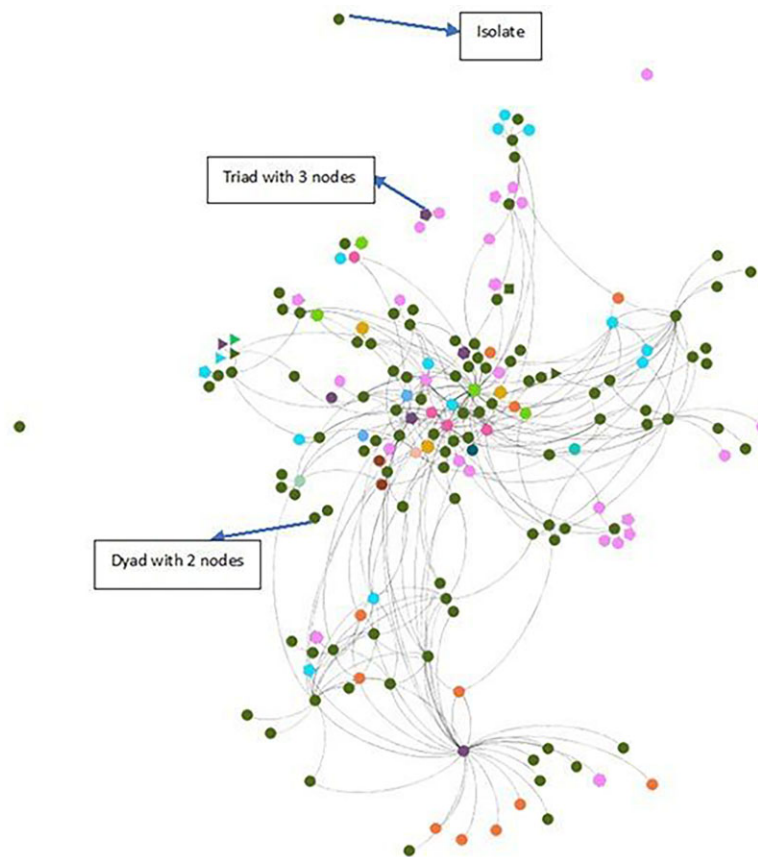
Figure 1: The interorganizational collaboration network ('which organizations within the HE sector have you collaborated with most frequently in the past year'). Colours represent different organizations and the shapes represent four different locations. The percentage of nodes by type is provided in Table 2.

ties, government bodies, colleges, public bodies, professional and industry groups, private sector organizations and non-profit organizations. We constructed a collaboration adjacency binary matrix (p = {pij}, i, j ∈ N) because, for this study, we are not interested in the intensity of the ties. The matrix contains in each row (column) the sender (receiver) organizations, and in the intersection cells (pij) the value 1 or 0 to indicate if they have shared cyber threat information from the row to the column organization. That means that the collaboration network is binary as it only shows the presence or absence of the ties and not the frequency or intensity of collaboration between nodes (organizations). It uses arrows to distinguish between the sender and the receiver in any information exchange. In these exchanges, reciprocity is not equal which results in an asymmetric network. That is, some organizations may *send* information but not *receive* it back, or the reverse.

A graphical visualization of the interorganizational collaboration network is shown in Fig. 1. A line representing the collaborative relations was mapped according to the responses of the participants who reported sending and receiving cyber threat information to and from other organizations in the network. Through observation of Fig. 1, we can see that the network is fragmented. Indeed, some organizations have no collaborative relationships at all. These are represented around the periphery of the main network and seen as isolated nodes (HEIs in green). We also see two smaller clusters; one represents a triad with three nodes where a non-profit education and training provider (light pink) is sharing information with two private sec-

tor organizations (purple) and the second shows two HE institutions (green) where one is sending out information to the other. Directly following on from Fig. 1 is Table 2, which provides the percentage of nodes separated by the type of organizations (e.g. institutional profile).

Qualities of the collaboration network
Table 3 provides the network level outcomes of the interorganizational collaboration network. We can see that the overall connectivity and cohesiveness of the network (density) is very low at 1.1%. This means that just over 1% of all the *possible* connections across this network of HEIs and relevant organizations are active. That is an extremely low finding and clearly demonstrates that collaboration in this sector in terms of sharing threat intelligence has significant scope for improvement. Indeed, we might say that existing collaboration in this network is negligible.

The network is highly fragmented
The *fragmentation* of the network is very high at almost 98%. This tells us that most nodes are not well-connected and that they are collaborating in silos or smaller groups rather than across the network as a whole. There were a number of comments about this in the interviews from people who participate in smaller sub-groups. One respondent referred to the Russell Group universities as a 'deep, historic collaboration' but also noted that with regard to cyberse-

Table 2: Percentage of nodes and organizational type

Organizational type	Colour code	% of nodes by type (%)
Universities		56.50
Public sector institutions		14.69
Government organizations		7.91
Colleges		6.21
Public private partnership		3.39
Non-profit organizations		2.26
Professional bodies		2.26
Unknown		1.69
Alternative educational providers		1.13
University group		1.13
Public sector bodies		0.56
Scottish HEIs		0.56
Welsh HEIs		0.56
Public limited companies		0.56
Other guild HEI		0.56

Table 3: Descriptive analysis for the network measures for the interorganizational collaboration network

Measure	Collaboration network
Density	0.011
Fragmentation	0.977
Arc reciprocity	0.300

Table 4: The top five organizations for receiving threat intelligence information from other nodes in the network

Organizations	Indegree
JISC	45
UCISA	23
NCSC	21
Microsoft	18
CISP	15

curity, they would recommend 'not being too exclusive and making sure that we collaborate across the HE sector' (Int1).

Information sharing is not reciprocal
Reciprocity in this network is also low at 30%. This means that 70% of instances of threat intelligence sharing are not reciprocated. That is not necessarily a negative indicator of network collaboration because a low reciprocity score could, e.g. arise from very proactive and effective information sharing by organizations intended to coordinate that collaboration. However, in this network that is not the case. Instead, the low reciprocity score reveals that information receiving nodes (in this case, those organizations we would expect to lead on collaboration) do not always send threat intelligence back to the nodes that share with them (the universities). Indeed, respondents say: 'It does not happen. Universities are truly awful at it. It is an ongoing topic of concern, not only in the universities but also with NCSC' (Int10) and 'we do not share very much with other folk' (Int9).

Who are the information consumers?
The *in-degree* measures the nodes that are most often selected for collaboration through sharing threat intelligence. JISC emerged as the most likely organization to *receive* information with 45 incoming ties. This was followed by UCISA, the NCSC, Microsoft and CiSP completing the top five which is referenced in Table 4. These organizations are regarded as 'trusted' by the network. Nodes are more inclined to share information with these organizations before other nodes. A visualization of the relationship between the five top organizations' high indegree centrality and collaboration behaviour is shown in Fig. 2.

Who are the information providers?
Table 5 shows the *out-degree* results for the top five organizations. The out-degree measures those organizations that most often share

threat intelligence across the network. We observe that all of the top five organizations for sharing threat intelligence information are HEIs rather than coordinating bodies like Jisc, UCISA or the NCSC. Indeed, there were no coordinating bodies represented in the top 10 rated for out-degree—all were HEIs. A visualization of the relationship between the five top organizations' high out-degree centrality and collaboration behaviour is shown in Fig. 3.

Where are the information bridges (and bottlenecks)?
Table 6 shows the results for *betweenness centrality*. Organizations with high betweenness centrality act as information bridges to other nodes in the network and again, the top five are all universities rather than coordinating bodies. These nodes are better able to manage and move information throughout the network. It is important to note that organizations that occupy this role also represent risk to the network. If they are prevented from sharing information (e.g. by their insurers or university management as discussed below), they can have a disproportionately negative impact on the whole network. They may even become an information 'bottleneck' rather than a 'bridge'. A visualization of the relationship between the five top organizations' high betweenness centrality and collaboration behaviour is shown in Fig. 4.

Where does the network go for information?
The *hub* ranking (Table 7) indicates those nodes to which other nodes are most likely to turn to for useful information. They can be equated to an administrator in an organization—they are most likely to be able to direct nodes to where they can *find* answers, but they do not necessarily *provide* those answers. A total of four of the top five organizations for this measure are HEIs but at number four is the Scottish Government. Our research revealed that the HE sector in Scotland is particularly cohesive and has a strong collaborative sub-network.
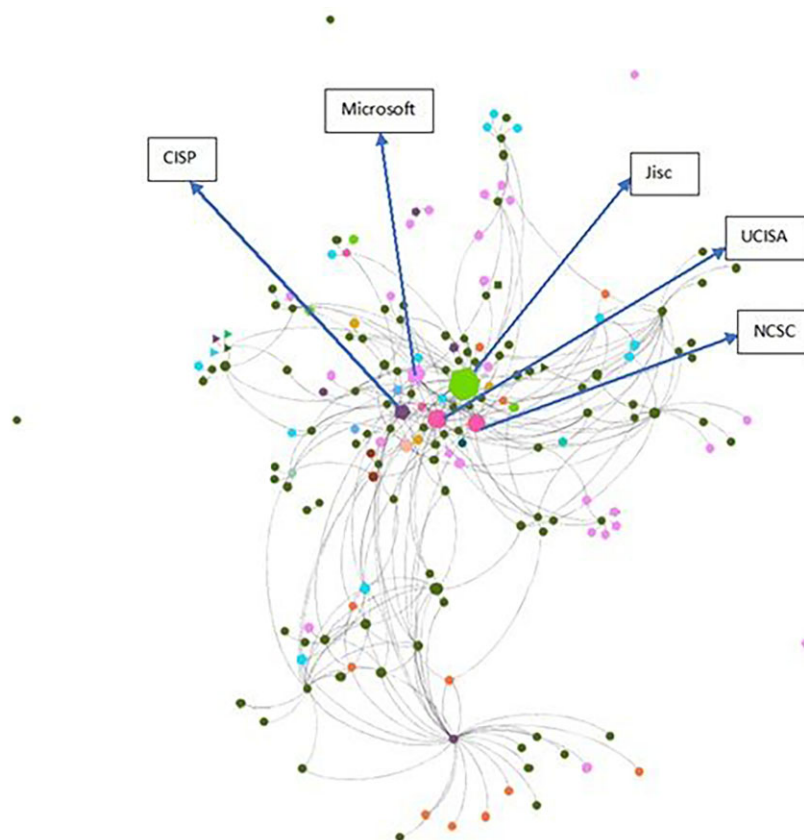
Figure 2: The visualization shows the nodes sized by in-degree. The top five nodes by size are named in the visualization. The shapes represent the location of the organization and the colour represents the institutional profiles.

Table 5: The top five organizations in the network for sharing threat intelligence information with other nodes in the network

Organizations	Outdegree
HEI83	29
HEI11	17
HEI58	14
HEI04	11
HEI35	9

They work closely with the Scottish Government, and this explains its high ranking as a hub in the overall network. This suggests that there may be lessons to be learned from the HE sector in Scotland that could be replicated elsewhere. A visualization of the relationship between the five top hub organizations and collaboration behaviour is shown in Fig. 5.

Which nodes are regarded as most authoritative?
Authority centrality (Table 8) is a measure of which nodes are regarded as having the 'right' information. Where a 'hub' node will be able to *direct* other nodes to where they might find answers, 'authority' nodes are understood to *have* those answers. The organizations with high authority centrality in this network include Jisc, UCISA, HEIDS, Microsoft and CISP. Notably absent from the top five is the NCSC, which came in at number nine after several HEIs. A visualization of the relationship between the five top authority organizations and collaboration behaviour is shown in Fig. 6.

Discussion of the SNA of this network

From the SNA, we see several patterns. For instance, the outdegree centrality measure shows the extent to which stakeholders in the sector are sending information out (or seen as 'information providers') to other nodes and we see that none of the organizations we might expect to do this in the network are in the top five. This includes Jisc, UCISA, Microsoft, CISP and NCSC. Instead, five of the total number of participating universities are found to play this pivotal role. The coordination bodies are predominantly operating as 'information consumers' receiving threat intelligence information shared with them by the universities but not reciprocating by sharing back (Fig. 7).

Betweenness centrality can be seen as akin to information bridges in our sample. Higher betweenness centrality identifies those organizations in the shortest path between nodes. These are organizations that have the propensity to connect different parts of the network thereby enabling a better flow of information across it. These nodes, if removed (e.g. by their senior management or insurance providers prohibiting them from sharing information) would lead to the network being further fragmented. These nodes (in this case, universities) act as influencers of information flow, and hence are important in ensuring that information moves across the network in a timely manner.

Receiving timely information is especially important as organizations will be more willing to collaborate and contribute threat intelligence if they are able to obtain actionable information. Information brokers or bridges are pivotal in a network as they connect members who are otherwise not connected [30]. Through the centrality analysis and understanding the role of these bridges, we can clearly
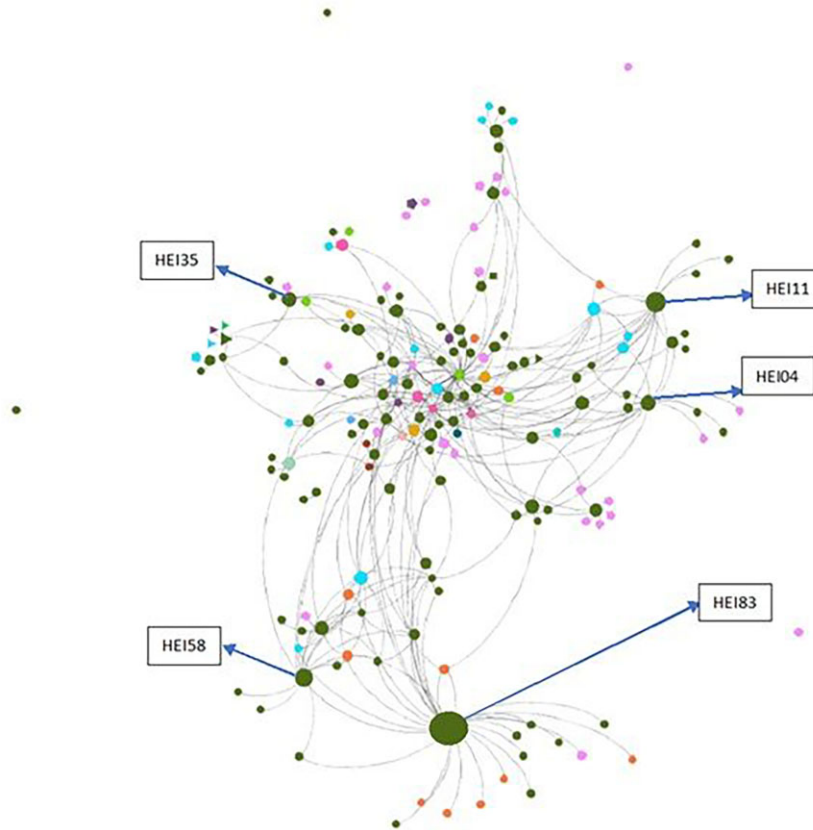
Figure 3: The visualization shows the nodes sized by out-degree. The top five nodes by size are named in the visualization. The shapes represent the location of the organization and the colour represents the institutional profiles.

Table 6: Betweenness centrality for the top 10 organizations in the collaboration network

Organizations	Betweenness*
HEI83	114
HEI11	72
HEI04	66
HEI58	51
HEI94	42

*Values rounded off to the nearest whole number.

say that in this network, it is universities that are currently acting as bridges and any changes that are to be led by sectoral bodies such as Jisc, UCISA or government bodies such as the NCSC, would need to go through these information brokers. They are not only relevant for sharing information but also for promoting and operationalizing the uptake of any new initiatives.

From the hub and authority analysis, it can be seen that, once again, universities play the role of key connectors. Hub nodes are considered to have the greatest impact as they have significant connections with several other nodes and usually point to the authorities in the network. It is interesting to note that the NCSC is not ranked high in terms of the authority value. This is because few nodes identified the NCSC as the organization they reach out to as a source of information. This is also substantiated in our interview findings where our research participants say that while the NCSC is an authentic information channel, sometimes their information is not very useful and is intended to benefit a more technical or operational au-

dience than CISOs. As suggested by one of the interviews: 'so, if you get something from the NCSC, it tends to be targeted directly at you as opposed to the industry as a whole. And then what they put out to the industry as a whole tends to be very generic, not very useful' (Int10). While the NCSC acts as the security point of contact for organizations in the UK, they will need to connect better and improve their reach to universities to go beyond providing technical guidance if they are to play a role in improving collaboration in this network.

Collaboration and the factors that limit it

The SNA of the UK HE sector reveals very low levels of collaboration (threat intelligence information sharing). Interorganizational collaboration has long been considered important in addressing these challenges [6, 31, 32] and *sharing sensitive information is strongly correlated with improved outcomes* for all [5]. Existing research has also shown that organizations that are isolated have a higher probability of being vulnerable to cyber-attacks and breaches [33–35]. In mitigating against cyber risks, collaborative arrangements support organizations to take integrative actions with the aim of collectively resolving a problem [36].

A cyber threat intelligence collaborative effort should include actionable intelligence from several sources, i.e. processed and sent to all organizations in a timely manner. It is important that there is integrated activity by organizations to ensure that the response to such threats is also coordinated [37]. A response coalition requires members to coordinate their activities and mechanisms to share intelligence in a secure manner [36]. Studies have shown that when orga-
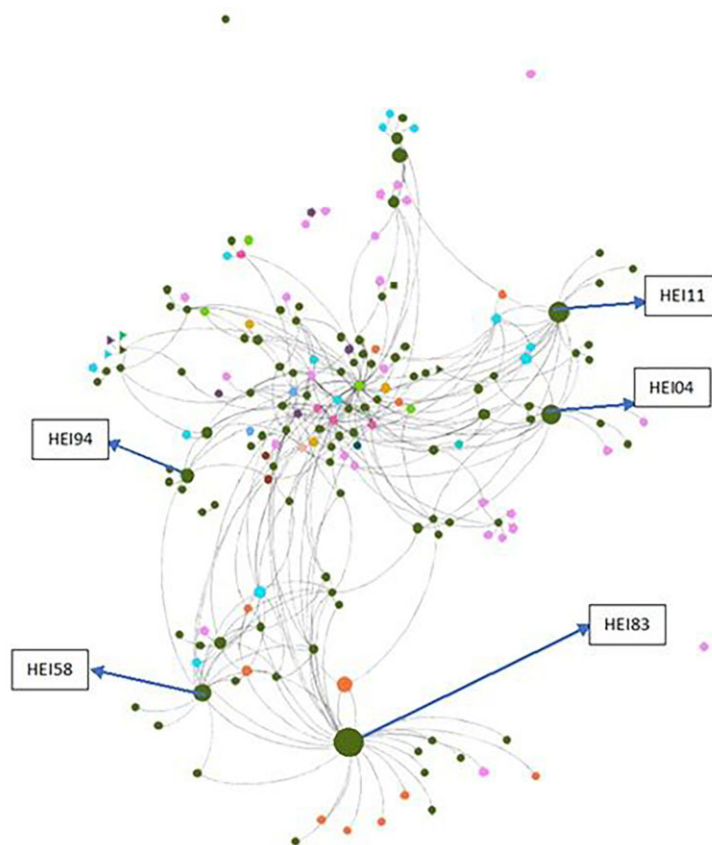
Figure 4: The visualization shows the nodes sized by betweenness. The top five nodes by size are named in the visualization. The shapes represent the location of the organization and the colour represents the institutional profiles.

Table 7: Hub results for the top five organizations in the collaboration network

Organizations	Hub
HEI83	0.289309
HEI35	0.242616
HEI105	0.229042
Scottish Government	0.224945
HEI207	0.215889

nizations are able to mobilize information and work collectively, this leads to effective threat responses [38]. However, while interorganizational collaboration has been demonstrated to be valuable, the main problem is that relevant intelligence has not been within the reach of most organizations. This is even more profound in the UK HE sector [39].

Given the challenges that the UK HE sector faces, the known benefits of collaboration on cybersecurity threat intelligence, and the fact that there are numerous organizing bodies within the network that could provide pathways for effective collaboration, questions arise as to why there is so little evidence of this across the network. In this next section, we present our findings on how the respondents perceived the benefits of collaboration and then what reasons they gave for the lack of it. We used a systematic, six-step process proposed by Braun and Clarke [40] for the thematic analysis of the qualitative data obtained through the interviews. In the first step, the researchers read the verbatim transcripts obtained to capture the meaning of

collaboration experiences of the participants. Secondly, initial labels were identified from these transcriptions and fed in NVIVO 12. The initial tags identified by the research team were then discussed, tags with similar meanings were merged before moving on to the third step, which was identification of the central and sub-themes. Once the themes were identified, for consistency, they were once again discussed and any overlapping themes were merged and duplicates removed in step four. In the fifth step, the macro-themes were described to recognize their meanings. Finally, the research themes were shared with the participants who reflected on their experiences to understand how well these themes captured what they had shared in the interviews. From the analysis, three macro themes were identified; relations, market forces and macro-environment. There were eight sub-themes, which are discussed below (Details provided upon request.).

Perceived benefits of collaboration
We asked our participants why they collaborated, and their responses were categorical. A significant majority of respondents agreed or strongly agreed that collaboration is a social mechanism that drives positive outcomes in the sector. In total, 94% of the respondents said that collaboration encourages mutual learning, 91% said that sharing cyber threat information encourages the development of solutions for cyber security problems, 81% said that the transfer of cyber threat information enables organizations to take collective actions and 95% said that the transfer of cyber threat information en-
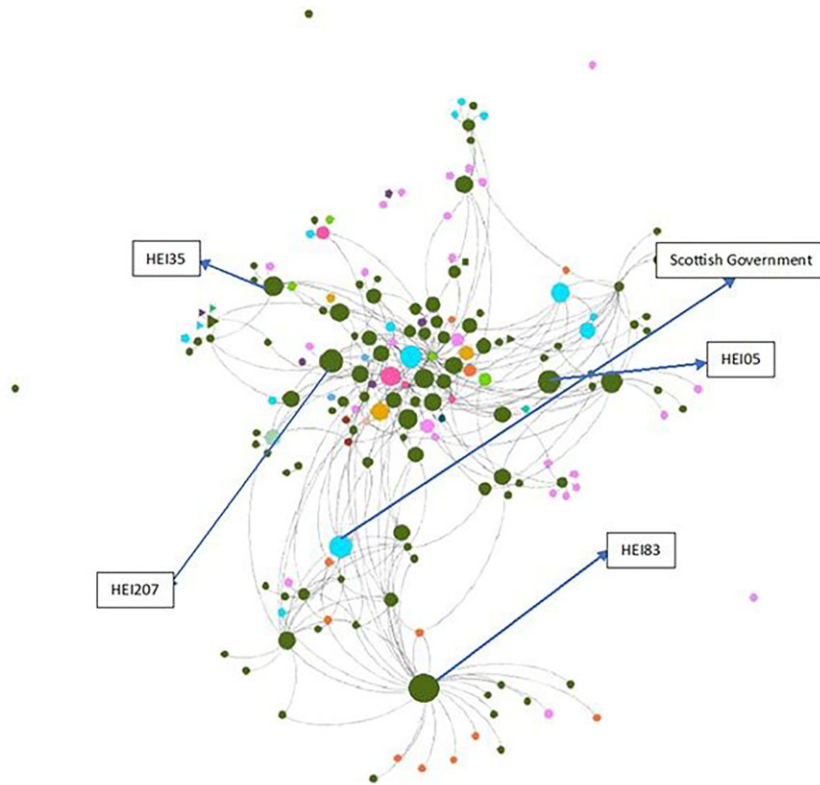
Figure 5: The visualization shows the nodes sized by hub centrality. The top five nodes by size are named in the visualization. The shapes represent the location of the organization and the colour represents the institutional profiles.

Table 8: Authority results for the top five organizations in the collaboration network

Organizations	Authority
Jisc	0.652577
UCISA	0.385627
HEIDS	0.382856
Microsoft	0.31049
CISP	0.25688

courages the development of a sense of community and fosters more integrated efforts to respond to cyber threats.

From our interviews, we also found a strong appetite for further collaboration in the UK HE sector. Respondents observed that universities are oriented around fostering the exchange of ideas and knowledge through collaborative relationships in the research sector and there was a perception that this would or should somehow organically extend to information sharing on cybersecurity. Some of the comments include '[our] institutions are naturally interconnected, [collaboration] is something we should be doing' (Int13). 'It is important to have a sense of community' (Int8). 'We collaborate on research projects, student exchanges, we share computing resources like HPC' (Int10). One respondent noted the benefits of 'the synergies of organizations trying to solve the problem at roughly the same time' (Int11).

Challenges to collaboration

The interviews raised five key factors that impede greater collaboration in this sector. We incorporated those factors into our question-naire to assess how participants viewed these five impediments. Some of the factors elicited significant agreement from the broader group while others were more contentious. Below is a figure that shows the results and in the following section, we discuss each of these five factors in more depth.

The role of trust

A lack of trust has been demonstrated to diminish the transfer of information [41].

In our questionnaire results, there were mixed responses to this factor. While a majority of participants neither agreed nor disagreed with the role of trust on collaboration, 15% agreed that a lack of trust was an impediment to collaboration and 10% disagreed with that statement. There were comments in the interviews about the need for a safe, secure space to share information—possibly anonymously. 'I think if it can be made clear that there is a safe environment that you can share this information in, that you will not find that someone from the *Mail Online* happens to be sitting in on that webinar or is logged into that particular forum, if you have got a controlled space that someone can provide assurance, 'This is a safe space and you can share information,' possibly anonymously, I think from a technical intelligence sharing information kind of perspective, that is really good' (Int2).

One factor may be that it is easier to share this information across smaller sub-networks. The SNA revealed that the ecosystem has very low levels of 'density', meaning that the overall network is not well-connected. Instead, nodes seem to cluster around smaller groupings like the Russell Group or geographic clusters as in Scotland. One respondent told us of an example in which a Russell Group university was being attacked and they '…shared immediately with the
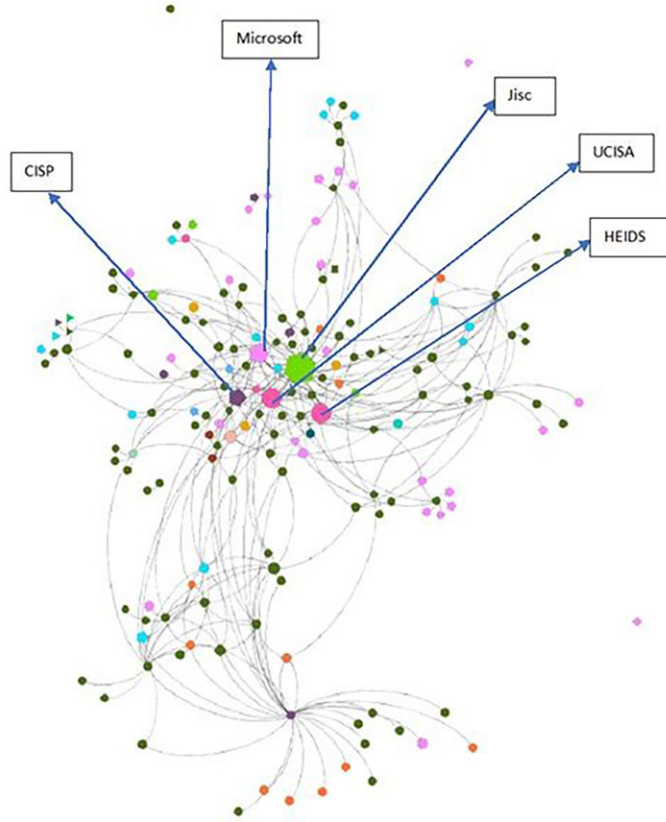
Figure 6: The visualization shows the nodes sized by authority centrality. The top five nodes by size are named in the visualization. The shapes represent the location of the organization and the colour represents the institutional profiles.
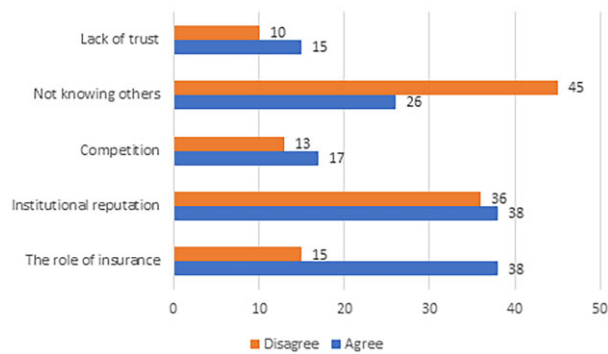

Figure 7: Obstacles to collaboration Note. Percentage of respondents reporting 1 or 2 (yellow) and 4 or 5 (blue), where 1 is strongly disagree and 5 is strongly agree.

[RUGIT] group the fact that they were under attack, what was happening. And there was lots of messages of support and help. There is nothing formalized yet in terms of how might we work together to help each other. But at least there is a level of trust, at least within the Russell Group, that this was being shared real time' (Int1).

Personal relationships

The development of trust between individuals as a factor in collaboration and information sharing has been established in a study by Tanczer, Brass, and Carr (2018) [42] that looked at international collaboration amongst the Cyber Security Incident Response Team

(CSIRT) community. The study found that people in the CSIRT community had close bonds with their colleagues and shared high value information with them. If their colleague left their post and moved to a new organization, that new organization would benefit from the information sharing and the old one would lose it. The information sharing followed the interpersonal relationships. Conversely, other research has established that the lack of trust can prove to be an obstacle to the exchange of information, and hence the development and the maintenance of collaborative trusted relations among organizations in cybersecurity settings is important to outcomes [41, 43].

Some of those who we interviewed would rather err on the side of caution than collaborate with a source they do not know or trust. They explicitly referred to interpersonal relations as determinants of information sharing. 'There are a few collaborators that we do have confidence in, and we can discuss things relatively openly' (Int14). And from another interview, 'we don't share information because of not knowing others personally—it is all about relationships. You know those relationships that are safe and those that are not' (Int3). A critical question remains then—how to develop institutional trust across the sector so that information sharing can transcend the dependence on individual personal/professional relationships which are, to an extent, transient. One study participant reflects this by saying that 'I would like to see us (as a sector) move towards a more trusting collaboration between ourselves' (Int17).

Competition

The role of market forces and competition was identified through our interviews as a factor that may limit collaboration, but it has also

been established in other studies [21]. However, this question elicited quite different responses in the questionnaire. Market competition within the sector was certainly perceived by some respondents as a barrier to information sharing. 'Competition plays a role in [the lack of] collaboration. I wouldn't be surprised if I find people thinking that one university losing a year's worth of students would provide opportunity for another' (Int10).

Other participants strongly refuted this view and did not regard competition between institutions to be a barrier to information sharing. 'We are not in a competitive environment like a business where we are all trying to make a profit from the same set of customers. Well, I suppose in one way we are, but we are not going to be withholding [threat intelligence information] because of a competitive edge' (Int4). Also, a degree of interdependence featured in responses to this question; '…we need herd immunity. If one institution is going to be attacked, we all are going to at some point' (Int10). This suggests that university management may wish to consider steering their CISOs away from a sense of competition and towards collaboration in order to best ensure their own institutional resilience.

Reputational risk

The issue of reputational damage also drew a lot of responses—both in agreement and disagreement. From the interview data, there were multiple complex dimensions to this that bring together concerns about institutional reputation, individual reputation and the risks of drawing attention to either one through acknowledging an incident. First, protecting the reputation of the university was a factor and second, the reputation of the individual was raised multiple times. Indeed, in some cases, the two appeared to be interrelated or even interdependent.

Some participants explained the effect of self-critical judgement when it comes to cyber attacks. 'When there is an attack you feel you have failed in some way' (Int14). Similarly, another interviewee comments 'Personal pride—if it is my job as an IT professional to safeguard something, I don't want to share my failures out to the world' (Int15). One interviewee also told us that 'in a technology world, you have a lot of technicians who are quite introverted who wouldn't want to go down that territory of sharing or admitting failure' (Int17).

Other respondents highlighted how concerns about institutional reputation can preclude collaboration. 'I firmly believe [protecting the] reputation [of the university] is the primary reason for not collaborating. Reputation underpins everything—if you have a bad reputation, no researcher wants to work there, nobody will trust you with their money or their data, no good lecturers and therefore no good students will want to study there' (Int9). This emphasis on institutional reputation and the links to damaging cyber incidents can inversely be perceived as a zero-sum game. One university's damaged reputation can present opportunities for others.

Significantly, there were other comments about reputation that linked back to the risk of escalating or prolonging an incident. One respondent pointed out that 'security is obviously a very sensitive subject. What you do not want to be doing is publishing your vulnerabilities' (Int1). Another told us that '…you don't want to say, 'we've been attacked and we've got over it and everything's fine,' because then they might just come and have another go' (Int3). And from the same respondent, '… you don't want to draw attention to yourself in the cyber world… if a cyber-attack occurs and you say that that's what's happened, then there is a fear that people would target you further' (Int3).

The role of legal bodies, university management and insurers

A significant number of the interview subjects (37%) raised the role of legal bodies and insurance providers as a factor that limits their ability to share cyber threat information across the sector. Multiple respondents commented along these lines saying that 'your insurers don't want you to share information' (Int10), 'you cannot share information during an ongoing investigation', and 'you get embroiled in the legal side of things' (Int 12).

University management also emerged as a blocker to further collaboration. 'I think a lot of the time people are not sure if they should [share threat intelligence], so they ask. And as soon as they ask, no one wants to say 'yes' because they are not sure. They do not really know what the implications of saying 'yes' are. And eventually it will get to someone in, you know, External Affairs and Communications or Media Group or whatever it is, and they will say 'no' because their concern is not [enhancing] sector wide intelligence and learning from other's mistakes. It has a reputational impact and managing the image of the university' (Int2).

Several respondents explained how they would avoid asking for permission to collaborate because they anticipate it would be denied. 'I did that post [sharing threat intelligence] anonymously because I want other people to benefit… [but] if I post something as a university of XXX employees, the university … may see that as an issue' (Int2).

Another respondent summarized what they see as quite different objectives and approaches from the IT/security staff in the university to the senior management and they commented on the impact this disjuncture has on further collaboration in the sector. 'I am hoping I do not have a significant breach, but if I do, I will be putting it all out there. And I do not think I will find any resistance from that within the university IT area. I think if someone feels they have to seek authority from higher up, the natural consequence is going to be that it will either be toned down hugely to the point where it is not useful disclosure any more or they will just say, 'Do not'. So, I will not ask because it is just easier. And again, that probably speaks to the level of understanding of the importance of IT and digital and cybersecurity at the higher level [of university management]. I think if people got how important it was, they probably would not object to people sharing anonymous but useful operational or information data' (Int2).

(Lack of) support and coordination from key organizations

While there was plenty of evidence throughout the data of a willingness to collaborate, there was also uncertainty about *how* to collaborate and which of the stakeholders should take a lead role. On whom should lead the way, opinions were divided as to whether collaboration would be most effective if led by universities themselves (as is now largely the case) or coordinated through existing sector specific bodies. One person new to the HE sector observed that the channels for collaboration and information sharing were not in place to the same extent that they had experienced in other sectors. 'Higher education tends to work independently. While there are a lot of industry groups on cybersecurity, this doesn't seem to be the case in the HE sector. We all share the same interests, and it is good to share but there's a lack of platform for someone like me who is new to the sector' (Int13). Another respondent new to the HE sector also expressed a preference for self-organized collaboration based on experience in other sectors. 'It would be really good if we could get to the point where we could create some kind of council. I call it that because we used to have an equivalent thing in government. So, you had the CIOs

and the CISOs of the main government departments, we'd all meet together regularly, and it would be a proper committee, with proper terms of reference, but no suppliers involved. And that's what I'd like to see in the sector. That would be my kind of mailing list' (Int5). To a certain extent, this already happens through the Russell Group IT network (RUGIT) but this sub-network was perceived by some respondents as too small and exclusive to bring about real change. 'A fragmented space kind of dilutes the benefit of sharing because you are actually only getting a sixth of the picture depending on which community you happen to be part of' (Int2).

Participants referred to several relevant industry stakeholders when it comes to sharing cyber threat intelligence information. Key amongst these were the Cyber Security Information Sharing Partnership (CiSP), UCISA and Jisc. There was positive feedback on CiSP. 'CiSP has the right amount of information—and … this has been a forum where people would start to talk' (Int10) and 'CiSP is being operated by NCSC, so you assume that the actual infrastructure of it is sound. It is secure, it is safe, it is trustworthy, and it is available to everybody that needs to have access to it' (Int9).

Other organizations were also positively represented in the feedback. 'Facilitating, collaboration and communication in the UK higher education sector around IT is what UCISA is all about' (Int7). 'I think Jisc and UCISA are both helping in this area across our sector. UCISA have certainly organized a few talks recently and got people like CIOs across the higher education involved in those' (Int13). UCISA was seen by some participants as the most likely forum for coordinating collaboration going forward. 'If you are looking at a structural facilitation of collaboration then it should be UCISA and I am absolutely certain that UCISA would put its hand up to help facilitate that, without a doubt. Facilitating, collaboration and communication in the UK higher education sector around IT is what UCISA is all about. And all of the networks are established to do that, all the communication routes, the lists, the information about who has which role, all of that is there' (Int7).

However, feedback on these stakeholders was not overwhelmingly positive. 'You could argue that Jisc should be in this space, but so far have shown themselves not to be' (Int7), 'Jisc is well-placed for this, they already have the network, they have all the mailing lists and they need to think of creating the community' (Int17), and '…nobody does anything useful in [UCISA]' (Int10). Jisc faced other criticism as a consequence of their emphasis on commercial service provision. 'Rather than just selling services, they [should] focus on putting together interest groups' (Int14).

The NCSC was also noted as having considerable scope for improvement, particularly in terms of sharing threat intelligence—the proxy in this study for collaboration. Comments included 'the NCSC could be more 'open' and 'consultative'—really difficult to get beyond the 'boiler plate' standard responses, especially when we ask for a situational update and we get someone reading from stock slides' (Int6), 'NCSC could take a more proactive role in terms of creating a sharing platform' (Int16) and 'the NCSC should play their part in sharing in advance the sorts of threats that we think we might be seeing in a few months' time. I am sure they have the ability to be able to know what is going on and what is likely to be attacking us' (Int12). This frustration at the inability to share more specific threat information is a common point raised by participants. The following quote is long but encapsulates many of the comments we gathered. 'So, there was a UUK conference on the topic, and three or four times me and others in the groups were saying, 'Can you give us an example of that? Can you tell us, you know, even an anonymized example?' And they just, you know the Government and the NCSC kept saying, 'We cannot talk about specifics. You have to share this amongst

yourselves'. And that is what led me to put the post up on CiSP to say, 'Look, we are going to have to share this amongst ourselves,' because you cannot go the NCSC and say, 'Well, what happened to [university x—redacted]? Was it a phishing email? Was it malware? Was it, you know, a trick bomb?' Whatever. You cannot ask them that because they cannot tell you. So, you have got to create that space where people can do it as peers. The take-up rate in CiSP seems to be very low in universities and possibly even nationally. I do not know. So, I think that needs to be addressed' (Int2).

Conclusion

In this study, we focus on the cyber security ecosystem in the UK HE sector by using a combination of SNA and qualitative analytical methods to ascertain how collaborative relationships function now, as well as what impediments and opportunities there are to improving this. Specifically, we find that there are currently very low levels of collaboration across the network, there is significant scope for coordinating bodies to positively impact this. University management also has a role to play in improving their own institutional resilience by removing impediments to threat intelligence sharing.

Organizations do not operate in isolation but are embedded in a web of relationships that provide opportunities and place behavioural constraints on employees. Collaboration is a relational process that can be captured in part through the study of cyber threat intelligence sharing networks. Through our combined methodology, we were able to describe a cyber threat intelligence sharing network and the sequence of pathways through which information is transferred among organizations in the UK HE sector. This has allowed us to make a number of recommendations.

From a research perspective, we argue that using this methodology can provide exceptional insights into other sectors or indeed, into the HE sector in other countries. By working closely with an industry body (in this case, UCISA), which was willing and able to facilitate our engagement with the sector, we were able to extract the volume of data necessary to make the study rigorous and the findings meaningful. The interviews helped us understand the sector well-enough to design the surveys and the SNA provided exceptional quantitative insights into where there is scope for improvement. Despite the positive inclination to collaborate of many of the study participants, the level of network fragmentation and the lack of coordination or support from external organizations is significant. Indeed, our research shows that existing collaboration across HEIs is negligible and only 1% of possible connections in this network are active.

The positive outcome of these findings is that there are concrete steps that can be taken to address this and that there is clearly significant scope to improve cyber threat intelligence sharing in the UK HE sector. From a university management perspective, there are three important findings. Despite competitive tendencies, senior managers can work to better support their cybersecurity teams to collaborate with peers in other universities. This will help to minimize the number of organizations that suffer from a particular attack and, in some of those cases, their own university will be the beneficiary of this collaboration. Secondly, senior management can clearly communicate to their CISOs that reputational damage (either for the institution or the individual) will not result from confidentially sharing appropriate threat intelligence with colleagues at other universities. And finally, there is a conversation to be had about the extent to which insurance policies can or should preclude this collaboration because it is currently detrimental to the security of the overall ecosystem.

The betweenness centrality rating highlighted that the information 'bridges'—those nodes in the network that are most important for capturing and disseminating information, are universities. Those information bridges need to be protected because disrupting them (e.g. by pressure from senior management not to share threat intelligence with other universities) would have a disproportionately negative impact on the whole network. As a consequence of this network relying almost exclusively on trusted personal/professional relationships, those information bridges are precarious and dependent on key actors identified.

While we find that there is lack of mature existing mechanisms for collaboration in this sector, there is also plenty of scope for organizations like Jisc, UCISA and the NCSC to improve this and one of our recommendations is that these bodies work together to honestly and openly appraise the scope of their existing and proposed services that they are able to put provide to the HE sector. It may be that some of these organizations, several of which originally emerged to deal with IT issues and have since grown to absorb cybersecurity, are not fit for this purpose. Defining the realistic scope of their individual, collective and combined remits would provide clarity for the sector. From our in-degree analysis, it emerges that sectoral bodies such as Jisc, UCISA and NCSC are pivotal and seen as 'trusted'. University CISOs are more likely to share information with them than with others in the network. However, the systemic failure of these organizations is highlighted by the out-degree rating as they are not proactively sending out threat intelligence to HEIs. These organizations are information 'consumers', but they are not information 'providers' and that may be because they do not have the necessary resources or capabilities. There should be a sector wide strategy to supplement these trusted relationships with an effective sharing platform that relieves the burden on key individuals.

Finally, there is an essential step that the UK research councils may wish to consider. Currently, a proportion of research funding goes towards university 'estates' but this refers to the university's physical estate. The last 2 years of enforced remote teaching will have lasting repercussions and the big lesson to come out of that period was that despite decades of investment in buildings, the university model of the 21st century relies much more on its digital estate than it does on its physical estate. Investment should reflect that through a proportionate amount of research funding to properly secure and support it.

There are a few limitations to this study to be acknowledged. While we have shown the inter-organizational network and highlighted the key actors in this sector, this study may be further enhanced by looking at organizational factors that *enhance* collaboration as well as those that *impede* it, as we have done here. In terms of future directions, we explain here how trust is one of the barriers to collaboration but, through the study, we also captured other networks such as 'advice' and 'best practice'. These would both be fertile areas for further research. The study looked at HEIs in the UK only. Some of the findings about the sector may be generalizable more widely but the biggest contribution beyond the UK is the methodology that could be replicated anywhere. We also note forthcoming work on the specific challenges that the UK HE sector faces with regards to cybersecurity.

This sector faces some unique challenges that, if shared in an effective, confidential way within the network, would allow for better coordination, shared lessons and coordinated responses. As universities become increasingly digitized and increasingly targeted by malicious actors, this collaboration will be key to ensuring growth, stability and security within the sector. And this, in turn, will be critical for the future of the UK as a 'science and technology superpower by 2030' [44].

Authors' contributions

Anna Piazza (Data curation [equal], Formal analysis [equal], Investigation [equal], Methodology [lead], Project administration [equal], Software [equal], Validation [lead], Visualization [lead], Writing – original draft [equal], Writing – review & editing [supporting]), Srinidhi Vasudevan (Conceptualization [equal], Data curation [equal], Formal analysis [equal], Methodology [equal], Project administration [equal], Software [equal], Validation [equal], Visualization [equal], Writing – original draft [equal], Writing – review & editing [supporting]), and Madeline Carr (Conceptualization [equal], Formal analysis [equal], Funding acquisition [lead], Investigation [lead], Methodology [supporting], Project administration [equal], Resources [lead], Supervision [lead], Writing – original draft [equal], Writing – review & editing [lead])

Conflict of interest

None declared.

References

1. NCSC. Further targeted ransomware attacks on the UK education sector by cyber criminals. 2021. https://www.ncsc.gov.uk/files/NCSC-Alert-Further-targeted-ransomware-attacks-education-sector-March-2021.pdf (30 April 2022, date last accessed).
2. PwC. Managing risk in higher education. 2021. https://www.pwc.co.uk/government-public-sector/education/documents/higher-education-sector-risk-profile-2021.pdf (1 May 2022, date last accessed).
3. Jisc. The future of employer-university collaboration—a vision for 2030. 2020. https://www.jisc.ac.uk/reports/the-future-of-employer-university-collaboration (30 March 2022, date last accessed).
4. Deloitte. The potential of partnerships. Higher education for a changing world. 2021. https://www2.deloitte.com/au/en/pages/public-sector/articles/higher-education-changed-world-university-industry-partnerships.html (31 March 2022, date last accessed).
5. Solansky ST, Beck T. Interorganizational Information sharing: collaboration during cybersecurity threats. *Pub Admin Quart* 2021;**45**:105–22.
6. Zhao W, White G. A collaborative information sharing framework for community cyber security. In: *Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST)*. p. 457–62. Manhattan, NY, IEEE, 2012.
7. Tagarev T. Towards the design of a collaborative cybersecurity networked organisation: identification and prioritisation of governance needs and objectives. *Fut Internet* 2020;**12**:62.
8. David DP, Keupp MM, Mermoud A. Knowledge absorption for cybersecurity: the role of human beliefs. *Comput Hum Behav* 2020;**106**:106–255.

9. Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. *Comput Secur* 2016;**60**:154–76.

10. Zhao W, White G. An evolution roadmap for community cyber security information sharing maturity model. In: *Proceedings of the 50th Hawaii International Conference on System Sciences*. AIS Electronic Library, 2017.

11. DiMaggio PJ, Powell WW. The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *Am Sociol Rev* 1983;**48**:147–60.

12. Zibak A, Simpson A. Cyber threat information sharing: perceived benefits and barriers. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. p. 1–9. New York, NY, Association for Computing Machinery, 2019.

13. Elwy AR, Kim B, Plumb DN. *et al*. The connectedness of mental health providers referring patients to a treatment study for post-traumatic stress: a social network study. *Adm Policy Ment Health* 2020;**47**:197–209.

14. Randall RG, Allen S. Cybersecurity professionals information sharing sources and networks in the US electrical power industry. *Int J Crit Infrastruct Prot* 2021;**34**:100454.

15. Wasserman S, Faust K. *Social Network Analysis: Methods and Applications*. Cambridge, Cambridge University Press, 1994.

16. Valente TW, Coronges KA, Stevens GD. *et al*. Collaboration and competition in a children's health initiative coalition: a network analysis. *Eval Program Plann* 2008;**31**:392–402.

17. Jasuja GK, Chou CP, Bernstein K. *et al*. Using structural characteristics of community coalitions to predict progress in adopting evidence-based prevention programs. *Eval Program Plann* 2005;**28**:173–84.

18. Mondada L. Challenges of multimodality: language and the body in social interaction. *J Sociolinguist* 2016;**20**:336–66.

19. Valente TW, Pitts SR. An appraisal of social network theory and analysis as applied to public health: challenges and opportunities. *Annu Rev Public Health* 2017;**38**:103–18.

20. Prell C. *Social Network Analysis: History, Theory and Methodology*. Newbury Park, CA, Sage, 2012.

21. Zrahia A. Threat intelligence sharing between cybersecurity vendors: network, dyadic, and agent views. *J Cybersecur* 2018;**4**:tyy008.

22. Borgatti SP, Everett MG, Johnson JC. *Analyzing Social Networks*. Newbury Park, CA, Sage, 2018.

23. Borgatti SP, Everett MG. A graph-theoretic perspective on centrality. *Soc Netw* 2006;**28**:466–84.

24. Kleinberg JM, Kumar R, Raghavan P. *et al*. The web as a graph: measurements, models, and methods. In: *International Computing and Combinatorics Conference*. p. 1–17. Springer, Berlin, Heidelberg, 1999.

25. NSCS. About the NCSC. 2022. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do (30 April 2022, date last accessed).

26. CPNI. About CPNI. 2022. https://www.cpni.gov.uk/who-we-are (2 January 2022, date last accessed).

27. UCISA. About us. 2022. https://www.ucisa.ac.uk/About-us (2 February 2022, date last accessed).

28. HEIDS. Higher education Information Directors Scotland. 2022. https://www.heids.ac.uk/ (11 January 2022, date last accessed).

29. EdTech. Why are managed service providers important for higher education. 2022. https://edtechmagazine.com/higher/article/2021/02/why-are-managed-service-providers-important-higher-education (11 January 2022, date last accessed).

30. Gehlert S, Carothers BJ, Lee JA. *et al*. A social network analysis approach to diagnosing and improving the functioning of transdisciplinary teams in public health. *Transdisc J Eng Sci* 2015;**6**:16–23.

31. Xie W, Yu X, Zhang Y. *et al*. An improved shapley value benefit distribution mechanism in cooperative game of cyber threat intelligence sharing. In: *IEEE INFOCOM 2020 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. p. 810–5. Manhattan, NY, IEEE, 2020.

32. Rodin DN. The cybersecurity partnership: a proposal for cyberthreat information sharing between contractors and the federal government. *Public Contract Law J* 2015;**44**:505–28.

33. Gylling A, Ekstedt M, Afzal Z, Eliasson P. Mapping cyber threat intelligence to probabilistic attack graphs. In: *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. p. 304–11. Manhattan, NY, IEEE, 2021.

34. Kirk R. Threat sharing–a neighbourhood watch for security practitioners. *Netw Secur* 2015;**2015**:5–7.

35. Mutemwa M, Mtsweni J, Mkhonto N. Developing a cyber threat intelligence sharing platform for South African organisations. In: *Proceedings of the 2017 Conference on Information Communication Technology and Society (ICTAS)*. p. 1–6. Manhattan, NY, IEEE, 2017.

36. Williams TA, Gruber DA, Sutcliffe KM. *et al*. Organizational response to adversity: fusing crisis management and resilience research streams. *Acad Manag Ann* 2017;**11**:733–69.

37. Drabek TE, McEntire DA. Emergent phenomena and the sociology of disaster: lessons, trends and opportunities from the research literature. *Disas Prev Manag Int J*. 2003;**12**:97–112.

38. Fraher AL. *Thinking through Crisis: Improving Teamwork and Leadership in High-risk Fields*. Cambridge, Cambridge University Press, 2011.

39. Chapman J. *How Safe Is Your Data?: Cyber-security in Higher Education*. Oxford, Higher Education Policy Institute, 2019.

40. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol* 2006;**3**:77–101.

41. Pala A, Zhuang J. Information sharing in cybersecurity: a review. *Decis Anal* 2019;**16**:172–96.

42. Tanczer LM, Brass I, Carr M. CSIRTS and global cybersecurity: how technical experts support science diplomacy. *Glob Policy* 2018;**9**:60–6.

43. . In: Bachmann R, Zaheer A. Cropper S. Trust in interorganizational relations(ed.), *Handbook of Inter-Organizational Relations*. Oxford: Oxford University Press, 2008.

44. Michelle Donelan and Rishi Sunak, UK Science and Technology Framework, Department for Science, Innovation and Technology, Prime Minister's Office, 2023. https://www.gov.uk/government/publications/uk-science-and-technology-framework (6 March 2023, date last accessed).