LSE Media and Communications

Media@LSE Working Paper Series

Editor: Bart Cammaerts

The State of Cybersecurity in Education:

Voices from the EdTech Sector

Velislava Hillman

The State of Cybersecurity in Education: Voices from the EdTech Sector

VELISLAVA HILLMAN[1]

[1] Velislava Hillman (v.hillman@lse.ac.uk) is a Visiting Fellow at LSE and founder of EDDS, where she leads an independent team of international experts providing comprehensive audit and evaluation of education technology products and vendors. As a researcher and academic Dr Hillman's work lies in education focused on the integration of AI systems into schools and the role and participation of children and young people in increasingly digitalised learning environments.

Published by Media@LSE, London School of Economics and Political Science ("LSE"), Houghton Street, London WC2A 2AE. The LSE is a School of the University of London. It is a Charity and is incorporated in England as a company limited by guarantee under the Companies Act (Reg number 70527).

ISSN: 1474-1938/1946

Other papers of the series can be found at:
https://www.lse.ac.uk/media-and-communications/research/working-paper-series

ABSTRACT

The growing dependence of K-12 schools (kindergarten, primary and secondary education) on digital technologies has led to increased cybercrime. Unlike other information and communication technology sectors, the EdTech industry tends to escape critical research enquiry. EdTech businesses work in a fast-paced, relatively unregulated environment and their cybersecurity measures remain largely unknown. Instead, the state of cybersecurity in K-12 education is often seen from the perspective of what the education community – teachers, school administrators, and students – does or doesn't do to prevent and minimise cyber insecurity. This paper focuses on the state of cybersecurity in education by bringing in two major stakeholders from the sector, namely EdTech businesses and organisations providing cybersecurity frameworks and standards, to map the challenges and identify potential ideal cybersecurity standard that meets the needs of K-12 education and prioritises children's data privacy and security.

1 INTRODUCTION

1.1 Research Rationale

The recent health pandemic propelled a rushed adoption of all kinds of education technologies (EdTech) in K-12 schools (kindergarten, primary and secondary education) globally. Besides the pandemic, policy, the digital technology industry, philanthropists, and venture capitalists have all played a role in legitimating digital schooling as an inevitable next step to innovating education. Yet, the impact of digitalising K-12 education remains contentious. Moreover, the digitalisation has also led to the growing risk of cybercrime.

The present study is an effort to take a step back and ask what is the foundation upon which EdTech platforms and applications are developed? Do they demonstrate robust security controls and ethical practices that prioritise children's best interests?

Increasingly, government policies are including the role of EdTech in K-12 education. At the same time, however, there is no government intervention in regulating a growing industry. Market forces alone don't incentivise the sector to satisfy the security demands of end-users. An alternative is to directly address the industry and collectively find the means to drive towards improvement that prioritises children and their education as soon as possible.

The level of cybersecurity EdTech vendors implement can be an indication that the concept of protecting the user (students and teachers) should be understood and addressed at a basic level. However, it would be a mistake to assume that quality security and privacy measures are designed by default in the world of business. Oftentimes, it is a matter of cutting corners, marketing, scaling, making a profit, and satisfying shareholders and investors – even merging with or selling to a bigger company (and leaving the fate of student data into someone else's hands). Therefore, the focus of this work is on the enterprise itself – the businesses providing digital tools in K-12 education – and its priorities towards children.

1.2 Theoretical guidelines

Platform studies (Poell, *et al*., 2019) and the economics of information security (Anderson & Moore, 2006) guide this research in two distinct ways. First, platform studies combine research perspectives from software, business, and cultural studies, as well as critical political economy (Poell, *et al*., 2019). Combined, these give platforms an institutional dimension which must be acknowledged along with the socio-technical and pedagogical transformation of education.

Derived from 'platforms' is the process of platformisation which comprises data infrastructures and data manipulation systems, markets, and governance, which can profoundly affect education, and the role and agency of its stakeholders. Moreover, schools' dependency on platforms and software applications to deliver, connect, communicate, assess, organise, analyse, recommend, predict, monitor, assign, manage, store, surveil, and so on continues to grow.

Platforms are also seen as intermediaries (Nielsen & Ganter, 2022) as their algorithms can adapt and influence the content and educational processes. They rank, procure, promote, and make available to students a constant flow and wide variety of content and choice of EdTech applications (e.g., see the digital learning platforms Clever, Knewton or Quizlet). Their intermediary role comes with power and privilege, and much like utility and infrastructure companies, they must have the responsibility and obligations to the public. In short, they require scrutiny and regulation. The need for scrutiny and regulation leads to the second theoretical guidepost of this research.

From information security economics, security failures in the digital domain can be seen as poor security investments and practices because of poor market decisions, the lack of policy incentives to prioritise cybersecurity, little cost-benefits (since cybersecurity measures are preventive, not motivated by profit), and overall lack of regulation.

The economics of information security aids this research in several ways. First, it helps to understand the factors that influence companies' decisions around cybersecurity measures and investments. Understanding the present state of the EdTech sector and the optimal cybersecurity investments for EdTech companies can inform, improve, or develop new and appropriate policies that can steer the sector to a 'race to the top'. Second, from technical point of view, security economics aims to drive the development of better security systems. Moreover, charting the state of cybersecurity in a digitalised education should encourage education stakeholders to move away from a culture of complacency about technologies and demand appropriate standards and quality. And third, the economics of security along with the platformisation of education demonstrates a sensitive dependability with many participants and no concrete responsibilities given to anyone. Policy development and government intervention should allocate responsibilities better to minimise and prevent the risks from cyber insecurity in education.

1.3 Implications of cyber (in)security to K-12 education

Cybersecurity attacks in K-12 education leads to all kinds of harm. They disrupt education; lead to loss of sensitive information about children and teachers; render systems unusable; some schools have even been forced to shut down (Collier, 2022).

Student data breaches, ransomware attacks, social media defacement, online class and school meeting disruptions are some of the incidents that affect education and individuals (Levin, 2022). In 2021, ransomware attacks cost $3.56 billion to schools in the US (Cyber Security Works, 2022). Between 2021 and 2022 around 41% of primary schools and 70% of secondary schools in the UK experienced cyber breaches (Department for Digital, Culture, Media & Sport, 2022). In the United States, Illuminate Education, an educational software, has gone through an avalanche of cyberattacks affecting the personal information of millions of current and former students (Singer, 2022).

As schools grapple with Covid-19 learning loss and growing expenses, the resources needed to protect against potentially destructive malware can be overwhelming. And while most literature, as evidenced in this work, focuses on what K-12 schools should do to protect themselves from cybercrime, the increased risks and negative impact of cyber insecurity is also linked to little regulation and scrutiny around the EdTech sector itself.

1.4 Cyber insecurities lead to data privacy risks and risks of harm to children

Risks of harm to children arise the moment data about them is collected by external entities with often unknown skills, capabilities, and motivations. Risks emanate from the development and deployment of advanced techniques and new models for data sharing and exploitation.

Cyber insecurities in the digitalised education can lead to both short- and long-term privacy risks of harms for students and teachers. Literature on the risks of harms from data privacy loss for individuals and societies abound (Brunton & Nissenbaum, 2015; Skinner-Thompson, 2021; Citron & Solove, 2022). The types of harms ensuing from data privacy loss can be physical, reputational, economic, discriminatory, psychological.

To the growing child, privacy plays a critical role in the development of feelings, ideas, and identity (Warren & Brandeis, 1890). Neil Richards (2008) calls intellectual privacy a "zone of protection that guards our ability to make up our minds freely" (p. 95). As K-12 education grows its dependency on EdTech platforms and applications, this zone of protection is increasingly determined by external forces. The loss of privacy leads to a wide range of risks

(Citron & Solove, 2021) whose sheer volume emphasises the need to ensure that all education stakeholders understand and prioritise children's data security and privacy protection. To this end, there is substantial gap in the literature as well as governmental scrutiny over the quality of EdTech products at their software foundation - cybersecurity.

1.5 Who is responsible for cyber (in)securities in education?

Some research outlines that K-12 education communities including teachers, school administrators, students, EdTech providers, and external malicious actors are all responsible for the digital (in)securities in education (Levin, 2022). Others (Fouad, 2022) emphasise that while K-12 schools and students tend to bear the cost of cyber risks, cyber insecurities are first and foremost a political and economic challenge.

Flawless cybersecurity, and with that 100% individual privacy, the industry may argue, is never achievable. As one senior engineer and the vice president of security of a US vendor said: "There's never a way to completely ensure privacy, only to control the risk associated with it."

However, this doesn't mean that liability should be left entirely to the end-user. Even if the industry bears the cost of cyber incidents, some argue (Kim et al.,2011) that the end-user will still pay the final (increased) price. In either scenario – whether industry or end-users bear the costs and liabilities – the risks of cybercrime remain. An alternative therefore is, as Fouad argues (2022), for government intervention by incentivising the sector to prioritise their cybersecurity efforts, by legislating security incident reporting, and by providing standards or models for security requirements that K-12 schools should look for when procuring EdTech products.

This paper continues with an overview of the methodology used followed by section three on findings from the scoping and review of literature and in-depth interviews. Section four provides recommendations and conclusion.

1.6 Methodology

Two methods were used for this study. First, in-depth interviews were carried out with industry representatives – EdTech founders, security and software experts, chief executives and/or technology officers. Interviews were also conducted with representatives of the National Cyber Security Centre (NCSC) and the IASME Consortium which provides the CyberEssentials cybersecurity framework, the National Institute of Standards and Technology (NIST) which provides the NIST cybersecurity framework (NIST CSF) and other frameworks (NIST 800-171/800-53), and the National Initiative for Cybersecurity in Education (NICE).

And second, publicly available literature (written in English), including policy documents, newspaper articles, and peer-reviewed papers, was analysed to identify the dominant discourse surrounding cybersecurity in education. From the period between February - September 2022, bi-weekly meetings were also held with the Global Education Security Standard (GESS) working group, an informal set-up, which included education stakeholders from Australia, New Zealand, the US, and the UK, during which discussions revolved around mapping and analysis of existing cybersecurity frameworks and which controls befit the EdTech industry and K-12 education.

The interviewed EdTech operators (table 1.1) were invited to participate in the research via the GESS working group networks, and by reaching out via social networks of various international EdTech alliances and hubs.

The conversations were audio-recorded, then transcribed and analysed using the NVivo software. Basing this research on grounded theory (Straus & Corbin 1998), selective coding and recording of the data allowed to develop key concepts and categories. These were shared with members of the GESS working group as a form of cross-checking since most members already worked in EdTech procurement and/or cybersecurity matters in K-12 education.

Table 1.1. *Description of participants*

Number	EdTech type[2]	Company size	Country /ies of operations
1	Platform, online learning environment and management system	Large (100+ employees)	USA, global
2	Online learning environment / application	Small (20+ employees)	UK, EU
3	Online learning environment	Start-up (between 1-10 employees)	UK, global
4	Application	Start-up (between 1-10 employees)	UK, EU
5	Application	Start-up (between 1-10 employees)	UK
6	Application	Small (20+ employees)	UK, EU
7	Online learning environment	Large (100+ employees)	EU
8	Online learning environment	Small (20 + employees)	Switzerland, Germany, Ukraine, USA
9	Online learning environment	Start-up (between 1-10 employees)	India
10	Platform	Large (100+ employees)	Japan, South Korea, EU, USA
11	Application	Start-up (between 1-10 employees)	Sweden, UK, EU, USA
12	Online learning environment	Start-up (between 1-10 employees)	UK
13	Application	Small (20+ employees)	Denmark, EU, UK, USA
14	Application	Start-up (between 1-10 employees)	USA, global
15	Management system	Start-up (1-10 employees)	Switzerland
16	National Cyber Security Centre (NCSC)	IASME Consortium ltd.	UK
17	National institute of standards in technology (NIST)	National Institute of Standards and Technology	USA
18	National Initiative for Cybersecurity Education (NICE)	National Initiative for Cybersecurity Education	USA
19	Vice president of cybersecurity and interoperability at an online learning environment	Large organisation (100+ employees)	USA
20	Digital learning environment	Large (100+ employees)	Netherlands, global
21	Publisher	Large (100+ employees)	Netherlands, global
22	Platform	Large (100+ employees)	Netherlands, global
23	Publisher and digital learning environment	100-250 employees	Australia, UK, USA
24	Digital learning environment and management system	Small (20+ employees)	New Zealand, global
25	AI-based tutoring system	Small (20+ employees)	New Zealand, global

[2] The names of the companies were omitted for confidentiality.

2 LITERATURE REVIEW

What the EdTech sector does to address cybersecurity challenges is largely understudied. Much of the existing literature looks at cyber incidents – how the education community is impacted and what schools and students should do to protect and prevent cybersecurity risks. Much less is said about government's role in scrutinising the EdTech industry. Having said that, the growing role of digital technologies in every sector and the explosion of internet-connected products, there has been an increased awareness and proposals for governance both from academia and various stakeholder communities. For instance, the forthcoming European Union cybersecurity rules will look at all internet-connected consumer products (European Commission, 2022). In the UK, the government cybersecurity strategy for 2022-2030 (UK Government, 2022) calls for developing skills and mechanisms for management and prevention of cybercrime. In the US, the ongoing revisions and updates around the cybersecurity legislature prepare for increased reporting and transparency (Bailey et al., 2022). On the other hand, others view the efforts at developing cybersecurity regulations to have become more complex, costly, and lacking harmonisation across jurisdictions (World Economic Forum, 2022).

2.1 Systematic scoping of literature between 2012-2022

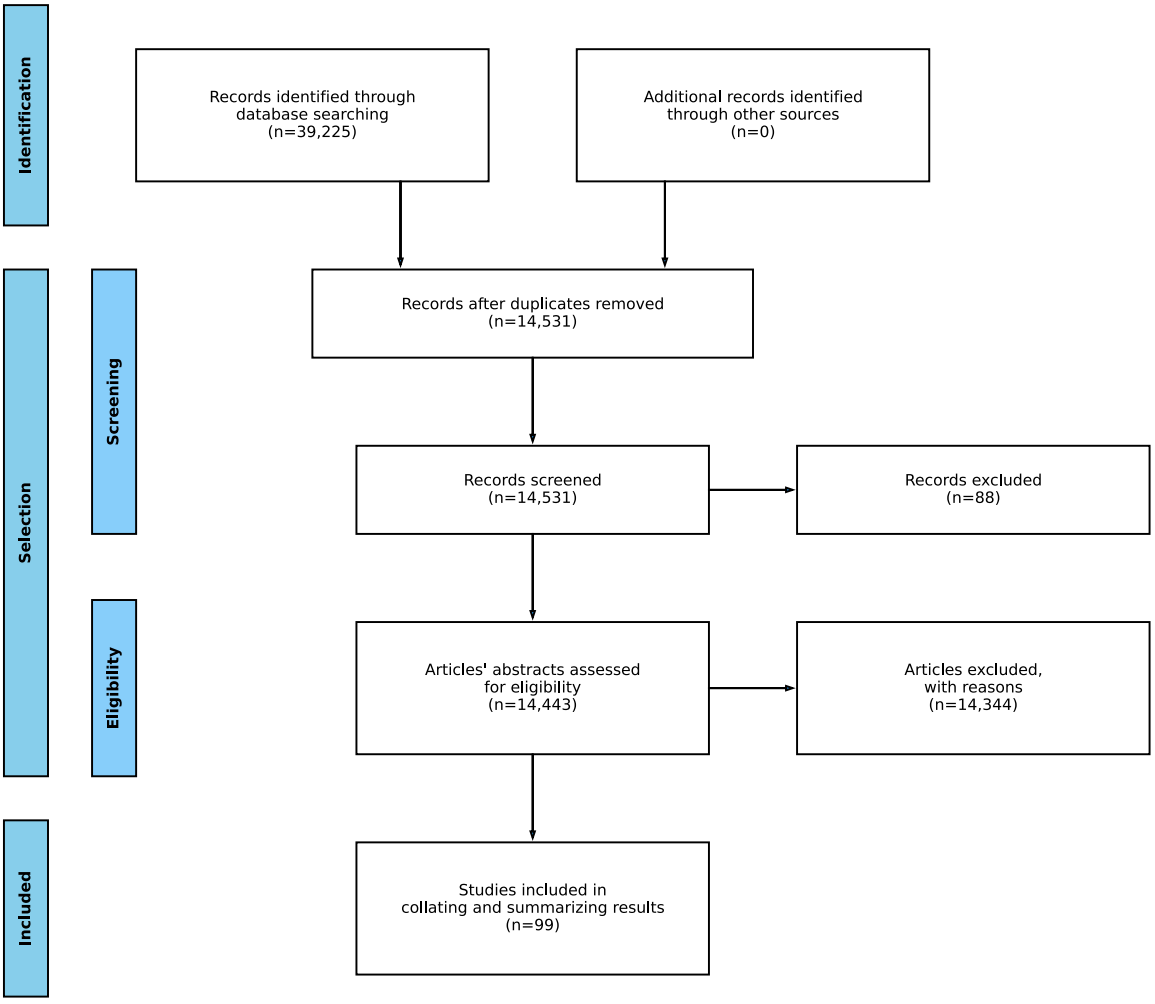
Systematic scoping (Zdravevski, et al., 2019) and thematic analysis were used to examine the dominant discourse within research about cybersecurity in EdTech during 2012-2022. The method utilizes Natural Language Processing (NLP) and automates the PRISMA meta-analysis methodology (Zdravevski, et al., 2019) to ensure an efficient and exhaustive search of the literature corpus in multiple libraries, namely, IEEE Xplore, Elsevier, MDPI, and Springer. This method generates detailed list of potentially relevant articles, trend charts over the defined time of interest, and a breakdown on various criteria.

A collection of initial keywords was used to identify potentially relevant articles (i.e., phrases that are used to query a digital library) and a set of properties that should be satisfied by the identified articles. The input is further expanded by proposing synonyms to the search properties. Duplicate articles obtained from multiple source libraries or searched keywords are automatically removed. Likewise, for fuzzy matching of search phrases and the actual titles and abstracts, the framework utilizes synonyms and stemming, so that the search is more robust.

Some properties could be denoted as mandatory or optional. The framework allows to discard articles based on some exclusion criteria (i.e., if they contain some phrases which identify

articles irrelevant to the study's goals). Initial keywords used to search through the libraries were given such as "cyber security in education", "cyber security AND education technologies", "cyber security AND education policy" and similar; in mandatory combination with others such as: "cybercrime", "policy", "principles", "law"; and other principal property groups such as "education technologies", "EdTech", "teacher cybersecurity skills", "malware", "malicious software", “end-users", “stakeholders", “pupils", and similar.

Figure 2.1 *PRISMA statement workflow with total number of articles for the present enquiry.*



Systematic scoping allows to automatically identify and process available literature, how the subject of cybersecurity in education is problematised, what knowledge base exists around the subject, how key stakeholders are positioned, and what responsibilities each stakeholder is given in these discourses. Full attention to the results of this methodology is beyond the scope

of this paper. Results and analysis will be presented elsewhere and in greater detail. The initial findings from this effort are shown in figures 2.1- 2.3.

The total number of relevant articles based on the enquiry about cybersecurity in education with regards to EdTech were 99. Unsurprisingly, a spike in literature appeared in the period of the pandemic – 2020-2022 – when most learning went online.

Figure 2.2 *Number of relevant articles for the past ten-year period from IEEE Xplore, Elsevier, MDPI, and Springer*

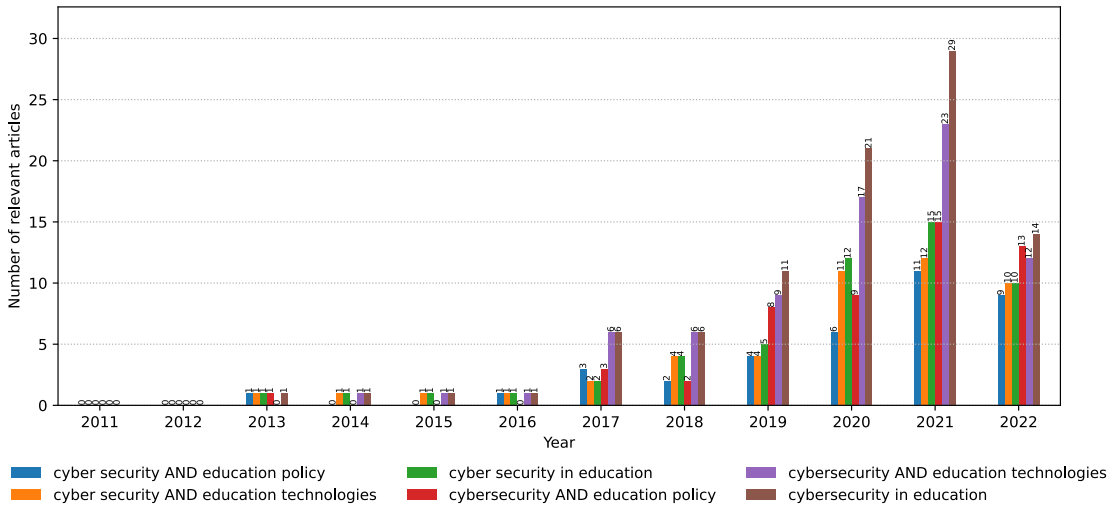
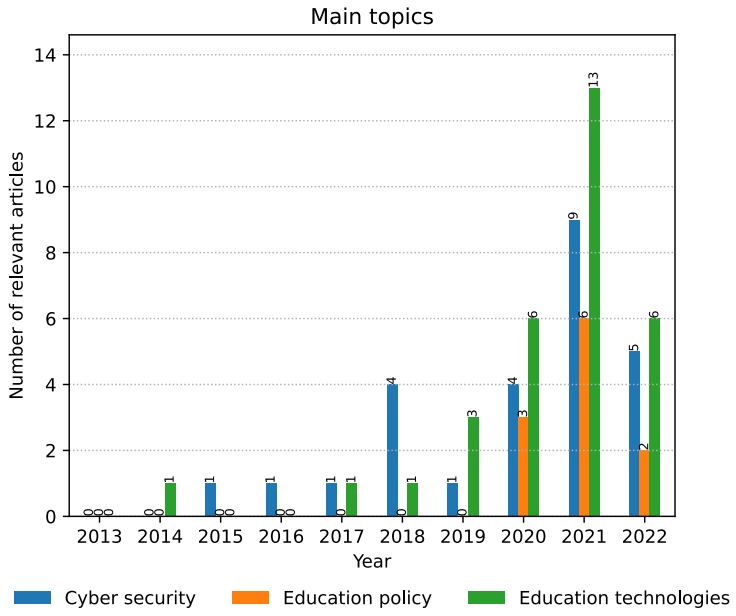


Figure 2.3 *Number of relevant articles based on the main topics of enquiry*



2.2 Literature skews towards the end-user's role in preventing cybercrime

Discourse around cybersecurity in education addresses more what the end-user (schools, teachers, students) should do rather than how policy and the EdTech industry can diminish and prevent cybercrime from disrupting and impoverishing children's education. Ironically, cyber criminals seem to remain faceless and in the margins of such discourse.

Some (Anderson et al., 2009) call this 'liability dumping' – shifting the responsibility of cybercrime onto end-users. Yet, research shows that around 80% of the software applications deployed by government and educational institutions use 'high-flaw density' and old codebases, while 23% of these have high severity flaws (Veracode, 2020).

Additionally, many of the technologies used in education are not even built with children in mind. During the pandemic, governments' recommendations to use Microsoft and Google products, originally designed for businesses, has led to normalising their use.

Government scrutiny escapes even those products that are specially designed for education. The recent massive data breaches of Illuminate Education affecting the personal information of millions of students, led to little more than their acquisition by Renaissance Learning, a learning and analytics company (Mollenkamp, 2022).

2.3 Cybersecurity is seen as an issue of lack of knowledge and competencies on the side of users

Some literature addressing cybersecurity in education also highlights the need for capacity building, education, and awareness among end-users (Calderaro & Craig, 2020); how school leaders "might effectively respond" to cybersecurity challenges in highly digitalised learning environments (Levin, 2021, p. 2); and the impact of cyber insecurities to education and children.

Scholarly work over the past few years has focused on developing cybersecurity awareness and curriculum for college students (Ahmad et al., 2021), educators (Ukwandu et al., 2020), and children (Maqsood & Chiasson, 2021).

Other research focuses on the effectiveness of information security programs in place within higher educational facilities (McClurg, 2015) and how to build resilience among students (Vain & Kharchenko, 2016). Yet others highlight that (lack of) knowledge among students is the main factor affecting cybersecurity behaviour (Kovačević, Putnik & Tošković, 2020), and that

teachers' skills and practices also impact the level of cybersecurity risks (Gallego-Arrufat, Torres-Hernandez & Pessoa, 2019).

2.4 Neither legislature nor economic motivations drive EdTech to prioritise cybersecurity

Some scholars observe that cybersecurity is economically challenging in the EdTech sector due to the lack of strong market incentives (Fouad, 2022) as observed from the discipline of security economics. While focusing on the Indian EdTech market, Fouad (2022) argues that the costs of cyber incidents tend to be transferred to the end-users and, due to the lack of mandates, there is little incentive for EdTech companies to prioritise budgets and efforts to increase the security of their products and services. This creates a "culture of acceptance for software and hardware insecurity" (Fouad, 2022, p. 264).

EdTech is a business like any other. Investing resources on cybersecurity is not seen as economically viable because its return is only measured through the minimising of risks and prevention of cybercriminal activities rather than an optimised or new feature that attracts sales or improves market position. Investing in cybersecurity controls and measures is therefore not seen as cost effective and it becomes of less priority to vendors (Böhme, 2013).

The review of literature has identified a substantial gap with regards to what EdTech companies do or are challenged by to prevent cyber insecurities in education. This gap is addressed next.

3 FINDINGS

This research started with the question: What cybersecurity frameworks and standards do EdTech providers adhere to? Some of the frameworks EdTech companies use for guidance include CyberEssentials (CE) in the UK, the NIST CSF, SOC2, and CSA STAR, and the ISO27002 standard. In Europe, the Directive on Network and Information Systems (NIS) is an EU-wide cybersecurity legislation which aimed to harmonize high-level national cybersecurity capabilities, cross-border collaboration, and the oversight of critical sectors across the EU member states (NIS Directive, 2016/1148). It addresses digital service providers of "essential services" such as transportation, banking, and healthcare but not, say, education;

it directs member states to comply "with international standards" (Article 16, NIS Directive, 2016, p. 21) but none concretely.

Seeking to move from theory to practice, ENISA, the European Union Agency for Cybersecurity, has also examined innovative engineering methods for data protection by design and by default (ENISA, 2022). However, it would be a daunting task to verify what (and if any) innovative techniques EdTech providers deploy to meet data protection principles the way it has been challenging to learn about what cybersecurity controls and frameworks the sector follows.

Existing frameworks are generally devised as a guidance for enterprises. CE, for instance, is a UK government-backed scheme which was developed by NCSC. Led by IASME Consortium, a private company, CE is an open framework, free for any organisation to use and self-assess. "Free", as the IASME Consortium representative explained, means that companies can internally put "essential cybersecurity controls" and carry on with their business.

> We're a group of 280 organisations licensed to certify businesses against the standard. With those plus businesses, there are 700 assessors in total. They can go out and advise on what to do and assess organisations. The key point to CE is around accessibility…If you want to get a badge that you have achieved those controls, there is a charge. For a small organisation it's £300 plus VAT, around £500 plus VAT for a larger organisation. A second assessment is an audited one. (personal interview, August 1, 2022)

There is a verified self-assessment which a company can submit. It can then be assessed by one of the certified assessors. Certified assessment can be done by another company. Then there is a second assessment – an audit. The company will still need to do a self-assessment, but the external assessor will visit the vendor site and check if the controls are implemented plus run an external vulnerability scan.

However, there are several challenges emerging from the present governing environment in the UK. First, there are no unique sector-addressing prerequisites (a standard?) that address the vulnerabilities of a digitalised K-12 education.

Certainly, educational institutions' priorities are to educate, less so to deal with encrypting data or server backups as much as they would need to deal with testing the school wall paint for lead. If educators show resistance against the added responsibilities, there should be other means to ensure that high quality EdTech products are used in their institutions.

Second, adopting the CE framework is voluntary. Although there have been some requirements from government departments, including the Department for Education, as the IASME Consortium's representative explained, it is not the business sector but local authorities, schools, and teachers who bear the burden of any issues relating to education,

including cyberattacks. Any effort on the part of government is at a basic level of communication and awareness, in the hope that industry will show good practice.

Third, self-assessment remains contentious with regards to the objectivity and quality of how and what controls are implemented. There simply is no way to know at what level of standard an EdTech provider is. As one UK vendor said: "I'll only find out when I've made a mistake". This trial-and-error attitude should not be allowed in K-12 education. There is a certain line of defence that data privacy officers provide in the UK (Hillman, 2022). However, there is a lack of robust evidence that privacy-preserving security controls are implemented across the sector.

Fourth, the assessors are companies which can certify others, possibly competitors, from the same sector. Companies from the finance, health, or education can become assessors and deliver certifications. Such trickle-down structure reflects the lax regulatory environment described by others (Mirrlees & Alvi, 2019). In a word, voluntary self-regulation remains industry's best practice.

In the US, NIST similarly provide a general security framework that does not target specific industry. Rather, it is "intended to be tailored or customised for a particular organisation or product or technology". However, as the NIST representatives explained, the biggest challenge remains how to support the small companies.

Presently, the NIST CSF framework is undergoing updates. As revealed, there is an interest to look at the demands of the EdTech sector servicing K-12 education. However, it would be anyone's guess what the update would look like. As the NIST representatives said, it will be "a little bit more digestible, and implementable to organisations of all different shapes and sizes". Like CE in the UK, however, NIST CSF remains a voluntary resource. The opportunity for an ideal scenario is up to companies to deal with and "every organisation has their own kind of risk appetite and risk tolerance".

Discussions around cybersecurity intersected with data privacy. There is "an increased sensitivity and compliance requirements for anybody who's a minor", as the representative of NICE pointed out, "the conversation has shifted to privacy, which is about safety, and not security just in the technical sense." However, separating data privacy and cybersecurity (that is "just in the technical sense"), becomes problematic for all stakeholders – educational institutions, policymakers, and industry. It fragments the problem of what should constitute 'quality' EdTech and blurs the roles and responsibilities of all stakeholders. In this regard, there is a gap among the existing cybersecurity frameworks in that there is no one comprehensive model, which details security controls and conditions that aim to meet data privacy requirements as enshrined in privacy laws, except for isolated efforts (e.g., the New

Hampshire Department of Education's House Bill 1612 [New Hampshire Department of Education, 2018], which has required "minimum [cybersecurity] standards for privacy and security of student and employee data, based on best practices, for local education agencies" [n. p.]).

Since some cybersecurity guidance is publicly and voluntarily available, it remains to be seen what the sector says about whether the current scenario works and for whom.

3.1 Feedback from the EdTech sector

There is no one sector-addressing cybersecurity standard designed to address the requirements and context of education and the EdTech industry. Having said that, lack of guidance does not justify free reign.

Smaller EdTech providers find it nearly impossible to achieve any cybersecurity controls that might be regarded as minimum standard (such as ISO27001/2). Most interviewed start-ups have not been assessed on any cybersecurity frameworks. In some cases, the existing standards like ISO27001/2 or NIST CSF, to many, seem "bureaucratic" and "tedious".

Others expressed the need for clear guidance on how to categorise the vulnerabilities and some sort of prioritising them for companies to know exactly where to focus on.

Being a global market, the EdTech sector sees the need for guidance especially because companies can move fast and get clients cross-border. A large US-based operator whose philosophy is "trust, but verify", said that it was challenging to satisfy all privacy laws and cybersecurity standards, suggesting:

> An ideal scenario would be to have cybersecurity standards that also cover data privacy laws and so it's all considered simultaneously. (personal interview, June 9, 2022)

Swiss EdTech companies grapple with a similar problem. Legal conditions are not only at national but also at Canton level. While EdTech vendors in Switzerland will address GDPR regulations and cybersecurity measures, the audits they undergo at Canton level tend to overlap. The "unnecessary redundancies", as one Swiss vendor puts it, tend to negatively affect the businesses – in some cases leading to business loss. The Swiss vendor also highlighted the discrepancy that exists between how start-ups are treated in comparison to big technology companies.

> Start-ups are heavily scrutinised. While for companies like Microsoft are somehow, you know, powerful and none of this scrutiny applies to them. I mean, they have tons of subcontractors in the US…while I am not allowed to use any subcontractors in the

> US…so it's a huge inconsistency in how those rules and regulations are applied. (personal interview, July 1, 2022)

Early-stage companies with less than five employees would find it near impossible to put any specific controls and be certified, first because of the huge cost and resources needed, and second because of the complexity of the existing cybersecurity frameworks.

3.2 The biggest challenges to meeting cybersecurity standards: costs and resources

Costs and resources required to meet security standards are the biggest hurdles for EdTech big and small. As noted elsewhere (Fouad, 2022), there is neither an economic incentive nor regulatory and policy intervention to rush the sector to cybersecurity responsibility.

The CEO of one US EdTech platform explained that while the costs can run up high, they are still not as high if an external party does the tests and assessments than if an internal individual runs everything. Moreover, internal assessments alone are like "marking one's own homework – it diminishes the overall trust".

> The assessments can be pricey - $50 000 from one agency [to make external cybersecurity assessments]. A third-party penetration test [external 'ethical' hacking of one's system], a three-year contract and multiple engagement of six assessments over the course of three years can be around $250 000. A SOC2 audit is about $60 000 for one that's just the capital cost that we may be paying. Then there's an internal training and expertise, putting in all the right controls. (personal interview, June 9, 2022)

Being new in the field is a challenge because small companies tend to be "IT under-staffed" as one Dutch EdTech vendor says, and because of the dynamic of how companies may change products, merge, or get acquired by others. This dynamic leaves no meaningful visibility to what needs a cybersecurity update or monitoring.

3.3 No cybersecurity mandates and low governmental (and often business) interest

There are no regulatory bodies to mandate or license EdTech operations. A Dutch EdTech vendor believed security around education data is not as "close to the bone" as, say, financial or healthcare data. The platform's senior engineer said:

> When profit is not involved, there is less interest from state power to monitor anything like this. So, it's like, companies that deal with education, if they're not too big, they don't think they'd be regulated. They care more about reputational hit. (personal interview, August 22, 2022)

This suggests a lack of awareness of the short- and long-term risks of harm from data privacy insecurities and loss for K-12 students. Therefore, there is a need for a systematic communication between the EdTech sector and K-12 education stakeholders, to highlight the risks of harm and ensure that EdTech representatives prioritise cybersecurity.

Cybersecurity risks also stem from the lack of timely security incident reporting. Without proper legislature to set the appropriate requirements, cyber insecurities in education will continue. If governments legislate security incident reporting and systematic assessments, it will undoubtedly nudge the sector in the right direction – sooner. Such shift of responsibilities towards the sector, however, is not enough, as some vendors pointed out. Schools, too, should play a role in setting up measures to prevent data breaches. A Dutch vendor said:

> A lot of data breaches come from accounts that are hacked, there isn't a good two factor authentication. You could limit that with 99%. And we find a lot of resistance from schools to implement that. The technology is there. We succeeded in implementing it in the secondary education; in primary education is still a struggle. (personal interview, August 22, 2022)

School district leaders and teachers are now thrust into an environment where they must quickly build often highly technical knowledge. As a US vendor's vice president of cybersecurity said:

> A lot of school districts don't know and don't have the expertise [in cybersecurity]. The person in charge of information security doesn't have direct training, right? They were never trained formally, in security and information technology and so on…they're thrust into an environment where now they're working with enterprise class switching and firewalling. (personal interview, September 26, 2022)

Aware of these challenges, the same respondent has also taken the initiative to not only provide a "workable" framework for schools to use when procuring EdTech products but has been organising training and support seminars. Such initiatives reflect a company's cultural ethos and duty of care. Nevertheless, this does not necessarily reflect the whole sector (at least it is hard to tell). Would then meaningful policies and mandates drive the market to maturity? There is a consensus among the respondents that a concerted effort in that direction is needed.

3.4 EdTech companies agree to a sector-specific cybersecurity standard

Generally, EdTech companies want to comply and have a better guidance about cybersecurity and other privacy preserving matters (taking response-bias in mind). However, there is also some pessimism as to how a standard can be achieved.

Most of the EdTech participants understood the vulnerability of their sector and showed willingness to take on measures that will guarantee them good practice. Vendors saw the risk of their own future if cybersecurity standards and data privacy were not met. As the US vendor's VP of cybersecurity said, "ultimately, customers will judge you by that [quality of cybersecurity]". The present dynamic of the sector is another sign that regulatory and policy measures are needed. The same respondent elaborated further:

> …I'll generalise this, you hire a bunch of young kids to do development. And they haven't been around the block a whole lot, right? They're right out of school…So, they write a programme that does the job. There's a lot of demand to get it out as quickly as possible. So, they release it. And then they're essentially using, you heard this before, that Apple uses their customer bases as a testing ground, right? … you need some people with maturity. I don't mean age, I mean, understanding of what's involved and where security needs to come in and how risk management is handled. And when you release something, what if it doesn't go right? Do you have a backup plan? Can you find a root cause? Can you do a "five whys" analysis? You need people that have that maturity level to govern the rest of the environment. And, yes, it's important to have those policies in place that require minimal standards. (personal interview, September 26, 2022)

Some vendors envisioned that cybersecurity matters or other benchmarks that can guide a minimum quality standard must ensure that they are tiered or flexible enough to apply to start-ups as well as established companies. However, a tiered approach would likely benefit mainly the industry (especially start-ups to give them the time to develop), not users. This would only increase the risks for K-12 schools in their limited capacity to understand and manage any residual risks (particularly, where a start-up may be offering a product that collects the most sensitive data such as behavioural, wellbeing, mental health, etc.). A security standard that has a tiered approach, therefore, should consider the inherent sensitivity of the data and functionality. Even with the best intentions to encourage innovation in the EdTech sector, companies must prioritise the safety and privacy of children.

A standard should not be seen as a static template but one that is refined all the time. As an Australian vendor said about the Australian, ST4S, framework:

> …they've been refining what they're doing over time. And you can see the work that they've put into it. Some of the provisions are new, but I don't think it's because the

> technology is new; it's because their awareness of what needs to be included is new. (personal interview, September 7, 2022)

A vendor from New Zealand providing AI tutoring looked at the lack of legislature and guidance as mainly a lack of expertise on governments' side. Ideally, the vendor believed, governments should do more and across the sector, to include the biggest players like Google, Amazon, and Microsoft, because users are becoming more concerned and aware of the risks relating to their data.

> Things like the fact that our data is in Europe is definitely preferable for our users, others ask and prefer that data states in our state or in their city and stuff. We're like, I'm sorry that's just not something we can provide at this stage. And often this is due to legislation. Maybe government's not really understanding the practicalities of trying to make this sort of stuff happen, and this disadvantages us. (personal interview, August 22, 2022)

There is growing awareness about cybersecurity risks in education among the education community and EdTech companies acknowledge that. However, as one New Zealand vendor said, "some [users] do ask where we keep the data and basic things like that but it's not a deal breaker".

Another key stakeholder in EdTech – investors and venture capitalists – also play a decisive role in what quality products enter the market. According to the interviewed participants, investors generally do not see cybersecurity assurances of significance. Most of the time, they do not even ask questions relating to cybersecurity and insurance. If they do, it is something "little on the side", as one vendor put it: certainly not a decision-making constraint. The reason behind it is financial (cybersecurity cost is spent on precautionary measures, not expecting to yield returns).

Despite the mixed responses, an ideal scenario emerged from the conversation with EdTech representatives, which is the focus of the next section along with the conclusion.

4 RECOMMENDATIONS AND CONCLUSION

EdTech companies are more understanding of the cybersecurity vulnerabilities in education and generally showed willingness to take on measures that will lead them to good practice. Most respondents were optimistic about having a standard, dedicated to the needs of K-12 education. The condition would be that a standard is at least flexible to accommodate start-ups and larger organisations. An ideal scenario could reflect some of the following recommendations, as the participants suggested.

- An ideal cybersecurity framework (standard?) must comprise security controls that underpin children's safety and data privacy.
- It should align with privacy laws that aim to protect children's privacy.
- Systematic and clear guidance should be made available (at a cost and resources proportionate to the maturity and size of organisations) to streamline good practices.
- To prevent "white-washing", such guidance should come with external validation through periodic and appropriate assessments.
- A "standard" should look like curriculum, whereby EdTech vendors "learn" (and implement) to pass regular exams.
- To work, a "standard" should approach companies through a tiered approach whereby a minimum tier prioritises student privacy and safety. A tiered approach will address companies' maturity. While this can expose the less mature, it ultimately enforces transparency about products and companies. As companies evolve and grow, so will the tiers of requirements and assessments.
- The internal organisational ethos and culture of EdTech companies must align with the priorities of K-12 education itself, which (should) centre around the protection of children's rights and freedoms and the delivery of quality education.
- Cultural change and capacity building is highly needed if a cybersecurity "standard" is to make a positive impact in the EdTech sector. Like healthcare professionals, software engineers and tech teams should understand the vulnerabilities in education, children's basic human rights and needs, and commit to safeguarding them.
- A "standard" should address the sector thematically: companies can implement controls and be assessed on those according to themes such as confidentiality (privacy), integrity, and accessibility – a triad that is the basis of development of security systems. On the other hand, this thematic model can be seen as too broad and equally too narrow as it cannot recognise the contextual nature of security (Lundgren & Möller, 2019).
- A "standard" can be tailored around concrete goals and functions: to govern, identify, protect, detect, respond, and restore.
- A "standard" should lead to consistency on the part of the whole sector.
- A "standard" should avoid redundancies (at regional level) to save resources, avoid protraction and therefore minimise risks.
- A "standard" should be an organic and evolving instrument that is regularly updated, involving industry and the education community; and maintain alignment with privacy laws.
- A "standard" should clearly articulate the risks and vulnerabilities around children's data in K-12 education and make these central for EdTech vendors' knowledge.
- The education community should have a practical version of the "standard" to support them in their understanding of what they can do to prevent cyber incidents, ensure data privacy, and aid procurement.

There are also several concerns that emerge from this research. These can be seen as points of departure for future work around protecting children's data privacy in K-12 education and, ideally, developing an EdTech sector-specific cybersecurity standard.

Some (Kim et al.,2011) argue that spending more on a mandatory standard can increase the cost of EdTech products, which schools would ultimately have to bear. While this argument didn't emerge from the discussion with the vendors, it is useful to mention it. Sifting through complex frameworks with several hundred questions, implementing controls and getting external validation incur substantial costs. However, as one vendor reasoned, "cybersecurity frameworks benefit the development of one's product and even start-ups can attend to these guidelines".

Many of the products are imposed on schools – they often cannot resist or refuse them. The post-pandemic reality can be seen as a surrender of schools to the institutionalisation of platforms and EdTech applications. This institutionalisation is demanding of the education community to adapt quickly and navigate through often highly technical challenges. No wonder much of the literature reviewed addresses the education community and the cybersecurity awareness and skills they need. School priorities are shifting from *what* one should be taught to *how* one should be taught with the range of EdTech products and technical risks they come with. However, cybersecurity responsibilities should be shared, and governments must ensure their fair allocation. Schools should neither bear the cost of *no* security nor for *more* security.

Government intervention for adequate measures of oversight is highly needed for the sake of protecting the K-12 education environment. The neo-liberal tendency to let the market sort itself out should be taken with caution. A case is made against government intervention because the EdTech sector is a relatively young and fast evolving. However, evidence has shown that self-regulation doesn't work. The rise of platform power increases the risks for individuals due to government inaction and outdated regulatory frameworks. Platforms such as Facebook and Google have grown powerful due to a combination of factors including the "inaction" from governments, "safe harbour provisions" protecting platforms from the "consequences of their users' actions ('intermediary liability exemptions')", data protection and privacy frameworks that fall behind technological innovations, and lack of authorities' attention over the potential of long-term harm from large scale-data collection (Nielsen & Ganter, 2022, p. 159). Self-regulation is created to deflect statutory control. Crucially, in the present context with the platformisation of children's education, self-regulation, government inaction, and inadequate regulatory frameworks should not be considered the norm.

Cybersecurity frameworks are guidelines; substantial maturity is required to navigate through them and deploy the right ones. Besides organisational and individual (e.g., developers)

maturity, cultural ethos and duty of care are also required from EdTech companies. Without incentives and appropriate level of scrutiny by governments, there is little guarantee for K-12 schools that EdTech companies would be aligned with appropriate cybersecurity benchmarks.

Technological challenges must be tackled first by those in the business of EdTech, the way pharmacologists and chemists have the know-how of what goes inside a pill.

EdTech providers acknowledge that schools have become more aware and demand to see companies meet adequate measures of data privacy protection and cybersecurity controls. That said, it is far from clear what questions should be asked and even how to request evidence that the right controls are implemented. The known frameworks contain hundreds of questions, many of which overlap. Written in highly technical language, not all of these are relevant to K-12 education. If many EdTech companies find it hard to navigate around these, how can one expect of schools to be able to?

Bringing cybersecurity up to standard for a start-up seems to carry no immediate cost benefit and doesn't seem like an urgent task in comparison to scaling up and more innovation. But this risky gamble shouldn't be at the expense of children's education and privacy. A way forward is to distribute responsibilities more fairly across the different stakeholders, including EdTech vendors. In that regard, the National Cyber Security Centre in the UK has proposed a cloud security shared responsibility model for companies who share part of their management to a cloud service provider (NCSC, n.d.).

However, there is much more to expect from a business sector whose influence in K-12 education continues to grow. Questions around cybersecurity and data protection only distracts away from the much harder work needed that is to nurture and raise bright and kind generations who can use all these innovative technologies for a good purpose. Adequate policies and regulation should come into the EdTech space soon, not only because of the harms that can ensue from poor cybersecurity and unethical practices, but also because children shouldn't pay for business mistakes with their own education.

ACKNOWLEDGEMENTS

This Working Paper exists thanks to all participants including EdTech vendors, the National Cyber Security Centre, IASME Consortium, the National Institute for Standards and Technology and the National Initiative for Cybersecurity in Education, and the GESS working group's leading entities – the Student Data Privacy Consortium in Cambridge, Massachusetts, the National Student Interoperability Program and Safer Technologies 4 Schools in Australia, and representatives from New Zealand's Ministry of Education. Special thanks to Annet Kloprogge, the Dutch EdTech group's managing director for her kind response and help with meetings and information.

I am thankful to all GESS members, contributors, and the leaders Steve Smith, CIO Cambridge Public Schools, Cambridge MA & Co-Founder of Student Data Privacy Consortium, Martin Rothbaum, Enterprise Architect, Te Tāhuhu o te Mātauranga at the Ministry of Education, Aotearoa New Zealand, and Anthony Yaremenko, Program Manager at the National Schools Interoperability Program, Australia, for their constructive feedback and support from the start of this research.

I am indebted to Dr Eftim Zdravevski for his help with the scoping methodology for the literature review. Special thanks to Prof. Nick Couldry and Mitzi László for their invaluable feedback around issues relating to education technologies, and for their friendship.

I wish to express my gratitude to Ronald Hepburn at Etoile Partners Ltd. for his trust and continuous support in developing EDDS and defending children's rights and freedoms in a digitalised education.

REFERENCES

Ahmad, A., Maynard, S. B., Motahhir, S., & Anderson, A. (2021). "Case-based learning in the management practice information security: An innovative pedagogical instrument." *Personal and Ubiquitous Computing, 25*(2021): 853-877.

Anderson, R. & Moore, T. (2006). "The economics of information security", *Science*, 314(5799): 610-13.

Anderson, R., Böhme, R., Clayton, R. & Moore, T. (2009). "Security economics and European policy", pp. 55-80 in Johnson, M.E. (Ed.), *Managing Information Risk and the Economics of Security*, New York, NY: Springer.

Bailey, T., Greis, J., Watters, M., & Welle, J. (2022, June 17). "Cybersecurity legislation: Preparing for increased reporting and transparency." *McKinsey & Company.* Available from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency

Calderaro, A., & Craig, J. S. A. (2020). "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building." *Third World Quarterly, 41*(6): 917-38.

Citron, D. K., & Solove, D. J. (2021). "Privacy harms." (GWU Legal Studies Research Paper No. 2021–11). *Boston University Law Review*. 1534: 1-60. https://scholarship.law.gwu.edu/faculty_publications/1534

Collier, K. (2022). "Illinois college, hit by ransomware attack, to shut down." *NBC News.* Available from https://www.nbcnews.com/tech/security/ransomware-attack-covid-combine-shutter-illinois-college-rcna24905

Cyber Security Works (2022, July 4). "Why should schools prioritise cybersecurity?" [Blog post]. Available from https://cybersecurityworks.com/blog/why-should-schools-prioritize-cybersecurity-1.html

Department for Digital, Culture, Media and Sport (2022). "Cyber security breaches survey 2022." *Department for Digital, Culture, Media and Sport*. Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064445/Education_annex_-_cyber_security_breaches_survey_March_2022__WEB_.pdf

Directive (EU) 2016/1148 of the European Union and of the Council of 6 of July 2016 concerning measures for high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p.1).

ENISA (2021). "Data protection engineering: from theory to practice." *European Union Agency for Cybersecurity*. Available from https://www.enisa.europa.eu/publications/data-protection-engineering

European Commission (2022, September 15). "State of the union: New EU cybersecurity rules ensure more secure hardware and software products." [Press Release]. Available from https://ec.europa.eu/commission/presscorner/detail/en/IP_22_5374

Fouad, N.S. (2022). "The security economics of EdTech: vendors' responsibility and the cybersecurity challenge in the education sector." *Digital policy, Regulation and Governance*, *24*(3): 259-73.

Gallego-Arrufat, M., Torres-Hernández., & N., Pessoa, T. (2019). "Competence of future teachers in the digital security area." *Communicar*, 27(61): 53-61.

Hillman, V. (2022). EdTech procurement matters: it needs a coherent solution, clear governance and market standards, Social Policy Working Paper 02-22, London: LSE Department of Social Policy.

Kim, B.C., Chen, P.-Y. & Mukhopadhyay, T. (2011), "The effect of liability and patch release on software security: the monopoly case", *Production and Operations Management*, 20(4): 603-17.

Kovačević, A., Putnik, N., & Tošković (2020). "Factors related to cyber security behaviour." *IEEE Access*, 2(1): 328-53.

Levin, D. A. (2022). "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report." *K12 Security Information Exchange* (K12 SIX). Available from https://www.k12six.org/the-report

Lundgren, B., & Möller, N. (2019). "Defining information security". *Science and Engineering Ethics, 25*(9): 419-41.

Maqsood, S., & Chiasson, S. (2021). "Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens." *ACM Transactions on Privacy and Security*, *24*(4): 1-37.

McClurg, J. D. (2015). *Cybersecurity in higher education: Oversight and due diligence* (Order No. 10291072). Available from ProQuest Dissertations & Theses Global. (1846958719). Available from https://www.proquest.com/dissertations-theses/cybersecurity-higher-education-oversight-due/docview/1846958719/se-2

Mollenkamp, D. (2022, August 29). "After recent high-profile data breaches, Illuminate Education quietly gets acquired." *EdSurge.* Available from https://www.edsurge.com/news/2022-08-29-after-recent-high-profile-data-breaches-illuminate-education-quietly-gets-acquired

National Cyber Security Centre. (n.d.) "Cloud security guidance: how to choose, deploy and use cloud services securely." *National Cyber Security Centre.* Available from https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model

New Hampshire Department of Education. (2018) *New Hampshire State legislature HB 1612* https://legiscan.com/NH/text/HB1612/id/1656674

Nielsen, R.K., & Ganter, S.A. (2022). *The power of platforms: shaping media and society.* Oxford: Oxford University Press.

Poell, T. & Nieborg, D. & van Dijck, J. (2019). Platformisation. *Internet Policy Review*, 8(4): 1-13 Available from https://doi.org/10.14763/2019.4.1425

Richards, N. (2008). "Intellectual privacy" (Working Paper). *Texas Law Review*, 87(1): 387–445.

Singer, N. (2022, July 31). "A cyberattack illuminates the shake state of student privacy." *The New York Times.* Available from https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html

Skinner-Thompson, S. (2021). *Privacy at the margins*. Cambridge: Cambridge University Press.

Straus, A., and J. Corbin. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* - 2nd ed. Thousand Oaks, CA: Sage.

UK Government (2022). *National cyber strategy 2022: Pioneering a cyber future with the whole of the UK.* Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

UK Government (2022a). *Government cyber security strategy: Building a cyber resilient public sector*. Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf

Vain, J., & Kharchenko, V. (2016). "Enhanced education for cybersecurity and resilience." *Information & Security: An International Journal,* 35(1): 5-8.

Veracode (2020), "80% of government and education sector software apps have flaws." Available at: https://www.veracode.com/press-release/80-government-and-education-sector-software-apps-have-flaws-sector-shows-progress

Warren, S. D., & Brandeis, L. D. (1890, December 15). "The right to privacy." *Harvard Law Review*, 4(5): 193–220.

Williamson, B., & Hogan, A. (2020). "Commercialisation and privatisation in/of education in the context of Covid-19." Brussels: Education International.

World Economic Forum (2022, March 28). "Why global harmonisation of cybersecurity would be music to everyone's ears." *World Economic Forum.* Available from https://www.weforum.org/agenda/2022/03/why-global-harmonisation-of-cybersecurity-regulations-would-be-like-music-to-our-ears/

Zdravevski, E. et al. (2019). "Automation in Systematic, Scoping and Rapid Reviews by an NLP Toolkit: A Case Study in Enhanced Living Environments.", pp. 1-18 in: Ganchev, I., Garcia, N., Dobre, C., Mavromoustakis, C., Goleva, R. (eds) *Enhanced Living Environments. Lecture Notes in Computer Science*, 11369. Cham: Springer.

The Media@LSE Working Paper Series:

- Presents high quality research and writing (including research in-progress) to a wide audience of academics, policy-makers and commercial/media organisations.
- Sets the agenda in the broad field of media and communication studies.
- Stimulates and informs debate and policy.

All papers will be published electronically as PDF files, subject to review and approval by the Editors and will be given an ISSN. An advantage of the series is a quick turnaround between submission and publication. Authors retain copyright, and publication here does not preclude the subsequent development of the paper for publication elsewhere.

The Editor of the series is Bart Cammaerts. The editorial board is made up of other LSE academics and friends of Media@LSE with a wide range of interests in information and communication technologies, the media and communications from a variety of disciplinary perspectives (including economics, geography, law, politics, sociology, politics and information systems, cultural, gender and development studies).

Notes for contributors:

Contributors are encouraged to submit papers that address the social, political, economic and cultural context of the media and communication, including their forms, institutions, audiences and experiences, and their global, national, regional and local development. Papers addressing any of the themes mentioned below are welcome, but other themes related to media and communication are also acceptable:

Communication and Difference	Mediation and Resistance
Globalisation and Comparative Studies	Media and Identity
Innovation, Governance and Policy	Media and New Media Literacies
Democracy, Politics and Journalism Ethics	The Cultural Economy

Contributions are welcomed from academics and PhD students. In the Autumn Term we also invite selected Master's students from the preceding year to submit their dissertations which will be hosted in a separate part of this site as 'dissertations' rather than as Working Papers. Contributors should bear in mind when they are preparing their paper that it will be read online.

Papers should conform to the following format:

6,000-10,000 words, 150-200 word abstract, papers should be prepared as a Word file, Graphs, pictures and tables should be included as appropriate in the same file as the paper, The paper should be sent by email to Bart Cammaerts (b.cammaerts@lse.ac.uk), the editor of the Media@LSE Working Paper Series

ISSN: 1474-1938/1946