Chapter 10

Cybersecurity in the Digital Classroom: Implications for Emerging Policy, Pedagogy and Practice

Alastair Irons and Tom Crick

Abstract

Recent cybersecurity education literature has focused on developments in cybersecurity curricula, qualifications and accreditation, pedagogy and practice to increase the number of cybersecurity professionals, in both the UK and internationally. There has been little research published to date on the online learning, teaching and assessment environment as a cyber target in its own right. This chapter appraised and discussed the dangers in, and emerging threats to, using online environments. It proposes a set of steps and mitigation measures that can be taken to make it more difficult for cybercriminals to attack educational institutions.

Keywords: Cyberattack; digital classroom; student credentials; online learning environment; security requirements; pedagogy; cyber policy

Introduction

The educational environment has changed radically – and will continue to do so – since the start of the COVID-19 global pandemic and the subsequent lock-down measures in every country and jurisdiction (Siegel et al., 2021a, 2012b; Shankar et al., 2021; McGaughey et al., 2021; Hardman et al., 2022; Watermeyer, Crick, Knight, & Goodall, 2021; Watermeyer, Shankar, et al., 2021). Combined with the demands of an increasingly digital, data-driven and computational world, there is a growing impetus for the evolution of the digital classroom, and especially digital pedagogy and practice (Crick, 2021; Watermeyer, Crick, & Knight, 2021). Pre-COVID-19, UNESCO identified the

The Emerald Handbook of Higher Education in a Post-Covid World: New Approaches and Technologies for Teaching and Learning, 231–244

doi:10.1108/978-1-80382-193-120221011

need back in 2008 that teachers should have the competencies to integrate digital technologies effectively into the curriculum (OECD, 2018), to help students develop the skills required for the twenty-first century, such as critical thinking, problem-solving and the ability to collaborate (Ward et al., 2021). Alongside this wider '21st century skills' imperative is the need to be aware of digital and cyber security threats from a societal, cultural and economic perspective (Tryfonas & Crick, 2015), linking to wider national and international shifts in computer science education (Brown, Sentance, Crick, & Humphreys, 2014) and digital skills reforms (Davenport, Crick, & Hourizi, 2020).

In this chapter, we pull together these key themes to look at the cybersecurity concerns associated with the modern digital classroom, the challenges (and opportunities) associated with developing the environment for a safe online teaching environment, and the cyber skills now required of both students and educators. In addition, we will explore the increasing value of academic records and student/institutional data to cybercriminals, and discuss the underlying motivations for why cybercriminals access educational systems. Whilst the emerging online classroom might appear to be a benign environment of little value to cybercriminals, we will discuss how online or cyber classroom environments can be exploited to become gateways to other institutional systems and educational data.

Tertiary education institutions (universities and colleges) across the world now find themselves rapidly moving into major programmes of digital transformation, both student-facing, and for their own systems, processes and infrastructure (Watermeyer, Crick, & Knight, 2021; Watermeyer, Crick, Knight, & Goodall, 2021 Shankar et al., 2021; McGaughey et al., 2021; Hardman, et al, 2022). Digital transformation is the process of adopting and using digital technology and data to deliver value and drive change (Branch, Burgos, Serna, & Ortega, 2020); in higher education, the emphasis is not necessarily on the use of specific digital technologies, but on the application of those technologies to support high-quality, pedagogically-driven learning, and teaching and assessment practice, as well as enabling wider transformational operational and organisational change. With the potential opportunities to embrace new ways of working as a result of the COVID-19 pandemic (Watermeyer, Crick, & Knight, 2021), especially from the rapid shift to online/hybrid approaches (Crick, Knight, Watermeyer, & Goodall, 2020, 2021), this has exacerbated the potential vulnerabilities in the emerging digital or cyber classroom (Renaud, van Schaik, Irons, & Wilford, 2020; Ulven & Wangen, 2021).

Educational environments globally have been transformed because of COVID-19 (UNESCO, 2021). In March 2020, as countries across the world went into various levels of lockdown and social isolation measures, higher education institutions moved quickly to find a solution to giving all students continued access to practitioners, learning materials and resources – the answer was 'emergency remote teaching', rapidly moving to an online or blended provision. Overwhelmingly, the speed of 'flipping to online' was clear, with faculty, tutors and professional services support staff rapidly redesigning learning, teaching and assessment (as well as implementing new systems, processes and infrastructure) to enable students to continue with their education (Crick, 2021; Crick, Prickett, & Walters, 2021; Irons, 2019; Watermeyer, Crick, & Knight, 2021; Watermeyer, Crick, Knight, &

Goodall, 2021). A further consideration of the lockdown environment is the fact that academics and students have been setting up and engaging with learning environments at home, away from the established systems and processes that would normally be in place in an institutional setting (Crick, Knight, et al., 2020; Watermeyer, Crick, & Knight, 2021; Watermeyer, Crick, Knight & Goodall, 2021).

Recent cybersecurity education literature has focused on developments in cybersecurity curricula (Association of Computing Machinery, 2020; Davenport & Crick, 2021), qualifications and accreditation (Crick, Davenport, Irons, & Prickett, 2019; Crick, Davenport, Irons, Pearce, & Prickett, 2019), pedagogy and practice (Crick, Davenport, Hanna, Irons, & Prickett, 2020; Irons, 2019) to increase the number of cybersecurity professionals, in both the UK and internationally (Irons, Savage, Maple, & Davies, 2016; Ruiz, Shukla, & Kazemian, 2020). There has been little research published to date on the online learning, teaching and assessment environment as a cyber target in its own right. In this chapter, we illustrate the potential dangers in using online environments, discuss emerging threats and suggest steps and mitigation that can be taken by practitioners and students to make it more difficult for cybercriminals to attack educational institutions.

Contextualising Cybersecurity in Educational Environments

In recent years – and certainly since the start of impacts resulting from the COVID-19 pandemic from March 2020 onwards – the use and application of computing technology and computer systems has experienced dramatic growth, particularly in education (Crick, Knight, et al., 2021; Luckin et al., 2013; Watermeyer, Crick, & Knight, 2021). The growth in the number of systems and the advances in the scale, functionality and usability of these systems have provided significant opportunities for malicious users to exploit insecure systems (Irons, 2019). The pace at which education providers and students have embraced technologies such as virtual learning environments (VLEs), online/blended learning and the use of smart devices, mobile technologies and the internet of things has rapidly increased the visibility and accessibility of digital educational environments, creating an education ecosystem that is changing faster than students, organisations and indeed legislators can often manage (Watermeyer, Crick, & Knight, 2021). It is not only the software and systems that are changing; the way in which students and faculty use the systems, with expectations of speed and convenience, means that cybersecurity can often be overlooked or secondary in importance to availability and interconnectivity. Allied to this growth in educational technologies is the growth in the amount of data that are generated at the individual and institutional level, and the variety of ways in which data are collected, stored, aggregated and manipulated.

The ways in which educational technology can be used in a university or college setting will vary depending on the students, level, subjects and disciplines, and the approaches that are used in designing and delivering courses. Typically, there will be universal access to a VLE, mediated by the university's security systems. However, the need for flexibility for both students and faculty means that there will often be add-ins to enable a range of functionality and features, including:

- editing of educational materials;
- links to video capture systems;
- embedding of third-party resources (including images, audio and video);
- access to library resources;
- submission of formative and summative student work in a range of formats; and
- provision of online feedback.

All the above are increasingly viewed as core features for a modern VLE, enhancing the range and accessibility of learning materials that can be developed for diverse student needs across a wide range of courses. However, all the above features listed are also potential weak points and vectors for attack in terms of cybersecurity and could be exploited by bad actors.

The wide range of software, systems and technologies – and the speed of their adoption and implementation – provides significant new opportunities for cybercriminals to exploit. In addition to taking advantage of existing vulnerabilities in systems, the advances in technology also provide the opportunity for cybercriminals to conceal their activities, to cover their tracks and attempt to destroy evidence of their actions. The ability to prevent or mitigate cybercrime attacks and cybersecurity breaches in the classroom has always been a challenge, but the speed of growth and the volume of activity mean that this challenge is escalating.

The nature of the diverse systems being used at universities and colleges means that there is a requirement for them to be interlinked and interconnected; for example, the need to link the VLE to the student administration systems and human resources systems in order to facilitate online learning and teaching operations. Whilst this enables online learning to be accessed by students and faculty, connecting these disparate systems potentially creates cybersecurity vulnerabilities; we will revisit this later in the chapter.

Every institution has a wide range of system functions; some used directly in the digital classroom, some to facilitate independent learning for students, and others to enable the 'business as usual' functionality of the institution. Many of these systems will be linked by function, but are also linked by technical architecture. There is a potential tension between accessing full functionality of the systems against the cybersecurity associated with the systems. In normal times, this would be considered as a vulnerability from a cybersecurity perspective; but in times when there has been a significant amount of rapid change with the adoption and use of digital technologies to allow students and faculty to participate remotely with online learning, teaching and assessment, the vulnerabilities are potentially exacerbated.

The changing educational technology environment and the growth in both explicit and potential threats mean that the role of cybersecurity in the classroom is increasing in importance. As educational providers globally become more reliant on utilising educational technology to deliver education, what we teach and how we teach it become key considerations. Similarly, there is a need to consider the students themselves, what they need and want to learn as well as how they learn about key cybersecurity principles in the classroom, irrespective of the subject that they are studying (Gupta et al., 2021).

An Emerging Threat Landscape

There are diverse sources of cyber threat in the digital environment and many of these threat sources could potentially relate to the emerging cyber classroom (Alexei & Alexei, 2021; Fouad, 2021). The education sector, across all settings and contexts (UK National Cyber Security Centre, 2021), is increasingly being targeted by cybercriminals due to the huge amount of sensitive data and in many instances relatively weak security infrastructure and implementations (Bandara, Balakrishna, & Ioras, 2021). Attacks can be both random or targeted – and it is targeted attacks on educational institutions that have increased in recent years, with the range of educational institutions being largely perceived as 'soft' targets (Alrabaee & Manna, 2021). Although the focus of this chapter is on cybersecurity issues in the classroom, and in particular, the emerging threats since the start of COVID-19, attacks on universities are certainly not new. These were early examples of motivation for cybercriminals to attack university systems: even during the early 1990s, a number of cyberattacks on universities were documented (Stoll, 1981). Universities had huge computer processing power, integrated and interconnected systems and external network links which provided direct access to a wide range of military and government systems. As well as access to processing power and gateways to external systems, the motivation for cybercriminals to attack these institutions includes access to other key systems, for example, finance, payroll, human resources and student data and the opportunity to catastrophically disrupt the core institutional business, for example, using the disruption to deny legitimate access and facilitate 'ransomware'. It is difficult to put accurate financial figures to the cost to educational institutions on these types of attack, but it is easy to see the wider impact to the UK economy from the annual Cyber Security Breaches Survey (UK Department of Digital, Culture, Media and Sport, 2021) conducted by the UK government.

Cyberattacks can come from a variety of different sources, with the nature of the attack and the attack vector varying depending on the attack type. Whilst the severity and impact of an attack will clearly vary depending on the specific circumstances and context, any cyberattack on an educational institution is going to cause an immediate disruption to core learning and teaching activities, and potential (digital) damage, and is likely have a longer-term financial and reputational impact (Venkatesha, Reddy, & Chandavarkar, 2021).

There are a variety of different threat vectors ranging from 'advanced persistent threats' typically funded by governments and nation states, through to hacktivists (often ideologically motivated) to nuisance threats (Alexei & Alexei, 2021; Venkatesha et al., 2021). Of course, there are also threats from organised cybercriminal groups who will exploit opportunities afforded by vulnerabilities in computer systems (Alexei & Alexei, 2021; Venkatesha et al., 2021). These attacks can be both computer dependent and computer enabled. A final group often identified in categories of attack vectors is often the most overlooked: the insider threat – these are unscrupulous, and often disgruntled, employees who will seek to cause disruption to their employer or find a way to make some personal gain (UK Department of Digital, Culture, Media and Sport, 2021; UK National Cyber Security Centre, 2021).

There are a number of points in educational systems that could potentially be vulnerabilities for attackers to exploit, including, but not limited to:

- hardware and infrastructure;
- software and integrated systems;
- connected university systems (e.g., finance, HR, etc.);
- VLEs;
- Email, instant messaging and connections to social networking;
- data storage (both personal and academic); and
- users.

Perhaps one of the most challenging threats to classroom security is human error. As institutions have rushed to provide high quality and comprehensive online and virtual learning experience for their students, it is easy to overlook the demands of robust, adaptable and verifiable security considerations. Especially as we try to put in place simple, accessible and usable solutions for diverse student groups. This is further exacerbated by academics and professional services staff working remotely from home and not having established university security systems and protocols in place, as well as the need for students to have frequent access to tutors, learning materials and online classes (Crick, 2021; Siegel et al., 2021a, 2021b; Watermeyer, Crick, Knight, & Goodall, 2021; Watermeyer, Shankar et al., 2021).

As well as the requirement to facilitate high quality and flexible online learning, teaching and assessment, being a new domain for educators and institutions, it also provides a new set of opportunities for attackers. Furthermore, cybercriminals have shown that they can be highly innovative and creative whist identifying targets to exploit (UK Department of Digital, Culture, Media and Sport, 2021; UK National Cyber Security Centre, 2021).

One current example of cybercriminal creativity is the use of ransomware attacks (UK Department of Digital, Culture, Media and Sport, 2021). Essentially, the attacks will utilise an attack vector to lock or encrypt so that the legitimate users will not be able to access systems or data. In order to obtain the 'key' to get access to systems and data, the attackers hold the education provider to ransom, hence the term ransomware (Fouad, 2021). Of course, this would be disruptive at any point in the academic year, for example, in blocking access to online classrooms or learning resources but can be particularly problematic in disrupting institutional business at key periods, such as enrolment or examination boards.

All of the high-level examples given in this section are potentially disruptive to the educational operations and core business of an institution, with associated financial and/or productivity loss; however, there is a further implication as a result of any cyberattack, system breach or data loss: reputational damage (UK Department of Digital, Culture, Media and Sport, 2021; UK National Cyber Security Centre, 2021).

A New (Ab)Normal for Education?

As we have indicated earlier in this chapter, COVID-19 has likely irrevocably changed the educational environment and ecosystem (Watermeyer, Crick, &

Knight, 2021; Watermeyer, Crick, Knight, & Goodall, 2021; Watermeyer, Shankar, et al., 2021). There has always been a digital aspect to education, especially since a diverse range of software and systems were systematically introduced to various levels of education from the late 1980s onwards. However, since March 2020, the speed of the shift to, and adoption of, various models of online learning, teaching and assessment has increased significantly (Gupta et al., 2021; OECD, 2018; Watermeyer, Crick, & Knight, 2021).

The widespread impacts of the COVID-19 pandemic, and especially the various 'lockdown' measures experienced in the majority of educational jurisdictions, meant that there was a rapid move to facilitate online delivery to ensure that students in all settings could continue to access education. Students expected to have immediate access to online learning and teaching, and to the full range of institutional software and systems (Watermeyer, Crick, & Knight, 2021). The uncertainty of working protocols at the start of the initial lockdown – and to which groups of society they applied – alongside preventing access to campuses with very little notice, meant that the infrastructure, architecture and access for the remote use of educational systems happened extremely quickly. There was a pragmatic requirement to ensure ease of access and minimal disruption to these systems for broad groups of academics, professional staff and students, giving rise to a particular set of challenges from a cyber security perspective.

The rapid move to online delivery meant that staff and students were routinely working from home or other locations outside of the standard institutional environment and access protocols. This led to a number of low-level security issues, including staff with a lack of IT expertise not going through appropriate checks and processes, and misconfiguring hardware and software (including downloading unapproved or potentially unsafe software) to access core institutional systems and specialist facilities to facilitate learning for students, with a marked increase in vulnerabilities and potential for attack.

Furthermore, with the rapid shift to online delivery came major institutional procurement, purchasing and licensing of new software, hardware and infrastructure. This meant rapid integration with existing institutional systems and data, providing remote authentication and access, largely without time to analyse wider security considerations or new threat exposure. The increase in the number of points of contact from staff and students meant that it was an increasingly complex threat landscape to monitor and to manage. Finally, whilst the majority of these were no doubt legitimate and credible, it also provided an opportunity for potentially unscrupulous hardware and software vendors to provide insecure or untested systems and create attack vectors in an educational enterprise-scale setting.

At the time of the first COVID-19 lockdown, during the 'emergency remote teaching' phase of the 2019/2020 academic year, there was concern about the ability to recruit new students for the 2020/2021 academic year. Many UK higher education institutions reviewed their financial positions and reduced expenditure, for example, major capital investments were delayed, new posts were put on hold, promotions cycles were postponed, pay increments were delayed (indeed, staff were asked to take pay cuts in some institutions to avoid any redundancies)

and all non-staffing costs were reviewed. Whilst there were immediate savings on travel costs and other types of routine expenditure, these did not offset the wider concerns about potential loss of income from student numbers, and especially international students coming to the UK. The core institutional spend on cybersecurity, often an area for debate before COVID-19, came under increased scrutiny. This was in the context of significant government and policy focus on the cyber resilience of higher education institutions from the UK National Cyber Security Centre, especially to protect strategic research and innovation investments and associated intellectual property, but also from a critical national infrastructure and economic perspective.

Discussion

Understanding the Value of Student Data

At first glance it may appear that student data may not have any immediate or exploitable value to cybercriminals. However, as with any sensitive personal data there is a requirement to protect and safeguard that data, especially under the requirements of UK data protection legislation. As highlighted earlier, educational institutions are increasingly subject to ransomware attacks; withholding access to or corruption of student and/or academic data would likely be a component of these types of attacks (Ulven & Wangen, 2021). Additionally, student personal data breaches may lead to various types of fraud, including identity theft; indeed, student data can be as valuable as financial data, used as a basis for obtaining false documentation and credentials and facilitating serious organised crime (Renaud et al., 2020).

Obtaining unauthorised access to student administration systems (required for online classrooms) can often be a gateway to obtaining privileged credentials for other institutional systems, for example, finance, payroll, procurement, HR, etc. One of the factors that make student data systems attractive to cybercriminals is that it is often difficult to detect when these systems have been compromised (Renaud et al., 2020). This means that attackers can have unrestricted access to the student data and related systems before institution or indeed student becomes aware of any issue. The problem can be further exacerbated if the educational establishment is not up to date in maintaining student records; for example, if a student withdraws from their course but the details are not updated it may be possible for the attack to 'cuckoo' and take over these records, continuing to receive student finance (Renaud et al., 2020). Similarly, if a student applies to an institution and is accepted but does not turn up to university to take up their position on a course, and never formally contacts the institution, a student record is created, which can be exploited for a range of benefits (Renaud et al., 2020).

Cybersecurity in the Emerging Digital Classroom

There are a number of cybersecurity issues in both online classrooms and indeed the traditional face-to-face classroom environments. As well as installing and implementing secure systems to enable the use of educational technology in the

classroom (Luckin et al., 2013), and collecting incredibly rich personal data on students (Williamson, Eynon, & Potter, 2020), there are various other factors which should be considered when considering cybersecurity in the classroom. All participants in the classroom learning environment, academic staff, professional services staff and students, should be aware of the increasing need for robust and adaptable cybersecurity in the classroom.

In order to embed effective cybersecurity in the classroom there is an expectation that the lecturer has a level of expertise and understanding of cybersecurity both in terms of the teaching environment and the context of the subject being taught (Crick, Davenport, Irons, & Prickett, 2019). In order for teaching to be effective it is important that the lecturer understands the level that students are at in their learning and also appreciate what it is students know about cybersecurity (Crick, Davenport, et al., 2020; Irons, 2019; Renaud et al., 2020). The tutor needs to be aware of the cybersecurity needs and the potential threats of attack in the classroom, as well as outside of the classroom. The question then becomes how much cybersecurity knowledge is required before using commonplace educational technology in a teaching environment. We also need to ask whether it is fair to expect academics to understand the diverse range of cybersecurity risks in a classroom environment, especially if they are not from a technical background or discipline.

Evidence suggests that many students consider the use of digital software, systems and online services as a positive environment, often without considering the explicit flaws or risks (Adorjan & Ricciardelli, 2019). Whilst this may be broadly helpful in facilitating learning and teaching, it often means that they do not think about wider security considerations, or how their student data could be compromised. It is important that all academics and professional services staff, irrespective of discipline or role, understand their responsibility in ensuring that both themselves and students understand the need for cybersecurity to be taken seriously in the online learning environments and settings (Admad et al., 2021).

Interestingly, a new online phenomenon was observed at the start of the emergency remote teaching phase in 2020: 'Zoom bombing'. This involved attackers who were not meant to be participants in an online classroom entering the classroom as unauthorised users and causing disruption, from sharing memes to sexist, racist and homophobic abuse (Renaud et al., 2020; Ulven & Wangen, 2021). There were widespread reported instances of these interruptions, both in the UK and internationally, leading to increased security settings and configurations for entry to online classrooms and the need for active management of online teaching sessions (Ulven & Wangen, 2021). Thus, to increase student awareness of the risks in the online classroom it is important for students to appreciate and understand:

- the need to be responsible digital users;
- the value of student data and their digital footprint;
- the wide range of potential threats and vulnerabilities;
- the need to recognise and validate trusted digital resources;
- the need to protect their digital devices; and
- the expectation as students to actively develop the positive and ethical use of academic software and systems.

Balancing Educational Needs and Security Requirements

In this closing section of the chapter, we indicate a number of key steps that can be taken to avoid online classrooms being easily compromised. As we have highlighted, it is important to get the balance right between ease of access to and use of the online classroom, as well as having in place the appropriate and necessary security measures.

There are a number of steps that can be taken to make it more difficult for attackers, including the following:

- Use high-strength encryption as much as possible (acknowledging it is not always feasible when running certain online classroom environments or activities).
- Utilise multi-factor authentication for entry into the classroom; whilst this might slow things down a little in terms of access to the classroom it is a very powerful technique in minimising unauthorised access.
- Apply the principle of least privilege: only enabling access to the online classroom when it is required, for specific roles and activities, and only for those academics and students who need access. Least privilege also means that access should be removed when access to the online classroom is not required.
- Related to this principle of least privilege, ensure that there is an end-of-life plan to manage access when students and staff leave (progression, graduation or otherwise), managing student records and ensuring that obsolete and unprotected equipment is decommissioned and removed.
- Constant vigilance (and do not be afraid to question or challenge): both tutors and students need to be aware of the environmental conditions and anticipated users in the online classroom, and when something does not look right they should be empowered to flag an issue or raise the alarm.

Although not directly linked to the online classroom, care should be taken when using official institutional email or messaging systems, as there are a number of classic exploits that cybercriminals will attempt to utilise. The main and well-known issue is 'phishing' and the closely-related 'spear phishing'. Phishing is when a cybercriminal tries to get a legitimate user to either pass information to the cybercriminal or get the legitimate user to click on an online resource that is controlled by the cybercriminal. In times of crisis, criminals often increase low-level phishing activity to target people as often their guard is lowered (Fouad, 2021; Ulven & Wangen, 2021). Common guidelines to staff and students at institutions to help protect against phishing scams may include the following:

- Are you expecting the email? If the answer is no, then please take additional care in opening or responding to the email.
- Is the language used in keeping with what is usual from the sender? If the answer is no, please take additional care and do not be afraid to contact the "sender" via another route to confirm authenticity.

- Hover over hyperlinks; do they link back to websites and email addresses that you recognise? If not, do not click them.
- If an email has an enticing offer associated with it and the offer seems too good to be true then it most likely is.
- Look out for misspellings in URLs and hyperlinks, particularly if these are close to legitimate ones, for example, www.sunderland.ac.uk is authentic, whereas www.sundreland.ac.uk is not.

Earlier in the chapter, we highlighted the multitude of issues emerging from the rapid move to online learning, teaching and assessment. In trying to find solutions to enable a useful, usable and manageable online classroom environment, academics should avoid signing up to 'free' services. Many of the free services which are frequently advertised are often restricted in functionality compared to the premium services (and are therefore not suitable for enterprise-scale installations), or often do not conform to UK data protection requirements and may potentially expose the institution to an unmanaged level of risk. It should also be noted that cybercriminals may use free software and services as a vector for collecting credentials so as to obtain privileged access to staff or student data. It is safer to use hardware and software that are institutionally approved and supported, meaning that due diligence and security checks will have taken place, adhering to the institution's security policies and processes.

Conclusion

Cybersecurity – and indeed cyber resilience – is a domain of growing interest and influence across all of our lives: across society, culture and the economy, and clearly from an educational perspective. In this chapter, we have highlighted and explored a number of key cybersecurity issues, concerns and threats with particular reference to the evolving online classroom, especially as a consequence of the rapid (and perhaps permanent, in some instances) shift to online learning, teaching and assessment. We have identified a series of potential threat vectors and modes of attack, and considered the reasons that educational institutions, academics, professional services staff and students could easily become the targets of cybercriminals and cyberattacks.

In a similar way to health and safety, cybersecurity is the responsibility of everyone; educational institutions, staff and students absolutely need to take explicit ownership for staying safe online; we thus need to create an engaged cybersecurity education community (Admad et al., 2021). As we have shown in this chapter, cybersecurity is an emerging and evolving challenge in education, and ensuring that people, data and systems remain secure and resilient will require constant attention and strategic investment. We all need to be vigilant, work together and do all we can to avoid the diverse landscape of vulnerabilities, exploits and attacks. Furthermore, we anticipate these themes becoming key future areas for research, policy and practice, as well as influencing learning, teaching and assessment across all educational levels.

References

Admad, N., Laplante, P., Defranco, J., & Kassab, M. H. (2021). A cybersecurity educated community. *IEEE Transactions on Emerging Topics in Computing*. https://doi.org/10.1109/TETC.2021.3093444

Adorjan, M., & Ricciardelli, R. (2019). Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. *Learning, Media and Technology*, *44*(4), 430–442. https://doi.org/10.1080/17439884.2019.1583671

Alexei, A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific & Technology Research*, *10*, 128–133.

Alrabaee, S., & Manna, R. (2021). Boosting students and teachers cybersecurity awareness during COVID-19 pandemic. In *2021 IEEE global engineering education conference (EDUCON'21)*, pp. 726–731. Piscataway, NJ: IEEE Press. https://doi.org/10.1109/EDUCON46332.2021.9454089

Association of Computing Machinery. (2020). ACM curricula recommendations. Retrieved from https://www.acm.org/education/curricula-recommendations

Bandara, I., Balakrishna, C., & Ioras, F. (2021). The need for cyber threat intelligence for distance learning providers and online learning systems. In *INTED2021 proceedings*, pp. 9312–9321. https://doi.org/10.21125/inted.2021.1947

Branch, J. W., Burgos, D., Serna, M. D. A., & Ortega, G. P. (2020). Digital transformation in higher education institutions: Between myth and reality. In D. Burgos (Ed.), *Radical solutions and e-learning. Lecture Notes in Educational Technology* (pp. 41–50). Cham: Springer. https://doi.org/10.1007/978-981-15-4952-6_3

Brown, N. C. C., Sentance, S., Crick, T., & Humphreys, S. (2014). Restart: The resurgence of computer science in UK schools. *ACM Transactions on Computer Science Education*, *14*(2), 1–22. https://doi.org/10.1145/2602484

Crick, T. (2021). COVID-19 and digital education: A catalyst for change?. *ITNOW*, *63*(1), 16–17. https://doi.org/10.1093/itnow/bwab005

Crick, T., Davenport, J. H., Hanna, P., Irons, A., & Prickett, T. (2020). Overcoming the challenges of teaching cybersecurity in UK computer science degree programmes. In *Proceedings of 50th annual frontiers in education conference (FIE'20)*. Piscataway, NJ: IEEE Press. https://doi.org/10.1109/FIE44824.2020.9274033

Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). A UK case study on cybersecurity education and accreditation. In *Proceedings of 49th annual frontiers in education conference (FIE'19)*. Piscataway, NJ: IEEE Press. https://doi.org/10.1109/FIE43999.2019.9028407

Crick, T., Davenport, J. H., Irons, A., Pearce, S., & Prickett, T. (2019). Maintaining the focus on cybersecurity in UK higher education. *ITNOW*, *61*(4), 46–47. https://doi.org/10.1093/itnow/bwz110

Crick, T., Knight, C., Watermeyer, R., & Goodall, J. (2020). The impact of COVID-19 and "emergency remote teaching" on the UK computer science education community. In *Proceedings of UK and Ireland computing education research conference (UKICER'20)*. New York, NY: ACM Press. https://doi.org/10.1145/3416465.3416472

Crick, T., Knight, C., Watermeyer, R., & Goodall, J. (2021). The international impact of COVID-19 and "emergency remote teaching" on computer science education practitioners. In *IEEE global engineering education conference (EDUCON'21)*. Piscataway, NJ: IEEE Press. https://doi.org/10.1109/EDUCON46332.2021.9453846

Crick, T., Prickett, T., & Walters, J. (2021). A preliminary study exploring the impact of learner resilience under enforced online delivery during the COVID-19 pandemic. In *Proceedings of 26th annual conference on innovation and technology in*

computer science education (ITiCSE'21). New York, NY: ACM Press. https://doi.org/10.1145/3456565.3460050

Davenport, J. H., & Crick, T. (2021). Cybersecurity education and formal methods. In *Formal methods – fun for everybody. Communications in Computer and Information Science* (Vol. 1301). Cham: Springer. https://doi.org/10.1007/978-3-030-71374-4_8

Davenport, J. H., Crick, T., & Hourizi, R. (2020). The Institute of Coding: A university-industry collaboration to address the UK's digital skills crisis. In *Proceedings of IEEE global engineering education conference (EDUCON'20)* (pp. 1400–1408). Piscataway, NJ: IEEE Press. https://doi.org/10.1109/EDUCON45650.2020.9125272

Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Gupta, R., Aggarwal, A., Sable, D., Chahar, P., Sharma, A., Kumari, A., & Maji, R. (2021). Covid-19 pandemic and online education: Impact on students, parents and teachers. *Journal of Human Behavior in the Social Environment*. https://doi.org/10.1080/10911359.2021.1909518

Hardman, J., Watermeyer, R., Shankar, K., Suri, V., Crick, T., Knight, C., McGaughey, F., & Chung, R. (2022). "Does anyone even notice us?" COVID-19's impact on academics' well-being in a developing country. *South African Journal of Higher Education*, *36*(1). https://doi.org/10.20853/36-1-4844

Irons, A. (2019). Delivering cybersecurity education effectively. In I. Vasileiou & S. Furnell (Eds.), *Cybersecurity education for awareness and compliance* (pp. 135–157). Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-5225-7847-5.ch008

Irons, A., Savage, N., Maple, C., & Davies, A. (2016). Cybersecurity in CS degrees. *ITNOW*, *58*(2), 56–57. https://doi.org/10.1093/itnow/bww053

Luckin, R., Bligh, B., Manches, A., Ainsworth, S., Crook, C., & Noss, R. (2013). *Decoding learning*. Nesta. Retrieved from https://www.nesta.org.uk/report/decoding-learning/

McGaughey, F., Watermeyer, R., Shankar, K., Suri, V., Knight, C., Crick, T., Hardman, J., Phelan, D., & Chung, R. (2021). 'This can't be the new norm': academics' perspectives on the COVID-19 crisis for the Australian University Sector. *Higher Education Research & Development*. https://doi.org/10.1080/07294360.2021.1973384

OECD. (2018). The future of education and skills: Education 2030. Retrieved from https://www.oecd.org/education/2030-project/

Renaud, K., van Schaik, P., Irons, A., & Wilford, S. (2020). *UK lockdown cyber narratives: The secure, the insecure and the worrying*. Available at SSRN. http://doi.org/10.2139/ssrn.3624789

Ruiz, N., Shukla, P., & Kazemian, H. (2020). Cybersecurity index for undergraduate computer science courses in the UK. *Journal of Applied Security Research*, *16*(4), 456–469. https://doi.org/10.1080/19361610.2020.1798173

Shankar, K., Phelan, D., Suri, V., Watermeyer, R., Knight, C., & Crick, T. (2021). "The COVID-19 Crisis is Not the Core Problem": Experiences, Challenges, and Concerns of Irish Academia in the Pandemic. *Irish Educational Studies, 40*(2), 169—175. https://doi.org/10.1080/03323315.2021.1932550

Siegel, A., Zarb, M., Alshaigy, B., Blanchard, J., Crick, T., Glassey, R., … Williams, D. (2021a). Educational landscapes during and after COVID-19. In *Proceedings of 26th annual conference on innovation and technology in computer science education (ITiCSE'21)*. https://doi.org/10.1145/3456565.3461439

Siegel, A., Zarb, M., Alshaigy, B., Blanchard, J., Crick, T., Glassey, R., … Williams, D. (2021b). Teaching through a global pandemic: Educational landscapes before, during and after COVID-19. In *Proceedings of the 2021 working group reports on innovation and technology in computer science education (ITiCSE-WGR'21)*. New York, NY: ACM Press. https://doi.org/10.1145/3502870.3506565

Stoll, C. (1981). *The cuckoo's egg; Tracking a spy through a maze of computer espionage*. London: Bodley Head. ISBN: 9780370314334.

Tryfonas, T., & Crick, T. (2015). *Smart cities, citizenship skills and the digital agenda: The grand challenges of preparing the citizens of the future*. UK Government Office for Science and Department for Business, Innovation & Skills. Retrieved from https://www.gov.uk/government/publications/future-of-cities-smart-cities-citizenship-skills-and-the-digital-agenda

UK Department of Digital, Culture, Media and Sport. (2021). Cyber security breaches survey 2021. UK Government. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

UK National Cyber Security Centre. (2021). Education and skills. Retrieved from https://www.ncsc.gov.uk/section/education-skills/schools

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039

UNESCO. (2021). COVID-19 impact on education. Retrieved from https://en.unesco.org/covid19/educationresponse

Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social engineering attacks during the COVID-19 pandemic. *SN Computer Science*, *2*, 78. https://doi.org/10.1007/s42979-020-00443-1

Ward, R., Phillips, O., Bowers, D., Crick, T., Davenport, J. H., Hanna, P., … Prickett, T. (2021). Towards a 21st century personalised learning skills taxonomy. In *Proceedings of IEEE global engineering education conference (EDUCON'21)*, pp. 344–354. Piscataway, NJ: IEEE Press. https://doi.org/10.1109/EDUCON46332.2021.9453883

Watermeyer, R., Crick, T., & Knight, C. (2021). Digital disruption in the time of COVID-19: Learning technologists' accounts of institutional barriers to online learning, teaching and assessment in UK universities. *International Journal for Academic Development*. https://doi.org/10.1080/1360144X.2021.1990064

Watermeyer, R., Crick, T., Knight, C., & Goodall, J. (2021). COVID-19 and digital disruption in UK universities: Afflictions and affordances of emergency online migration. *Higher Education*, *81*, 623–641. https://doi.org/10.1007/s10734-020-00561-y

Watermeyer, R., Shankar, K., Crick, T., Knight, C., McGaughey, F., Hardman, J., … Phelan, D. (2021). "Pandemia": A reckoning of UK universities' corporate response to COVID-19 and its academic fallout. *British Journal of Sociology of Education*, *42*(5–6), 651–666 https://doi.org/10.1080/01425692.2021.1937058

Williamson, B., Eynon, R., & Potter, J. (2020). Pandemic politics, pedagogies and practices: Digital technologies and distance education during the coronavirus emergency. *Learning, Media and Technology*, *45*(2), 107–114. https://doi.org/10.1080/17439884.2020.1761641